

## Data Processing Addendum

This Data Processing Addendum ("DPA") is incorporated into and supplements the Agreement, as updated from time to time between the Clarivate entity that is a party to the Agreement (together with its Affiliates, "Clarivate") and the Client entity that is a party to the Agreement ("Client" or "you").

Client enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates if and to the extent Clarivate processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Client" shall include Client and Authorized Affiliates.

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. For the avoidance of doubt, all references to the "Agreement" shall include this DPA, including the SCCs (where applicable), as defined herein.

### 1. Definitions

- (a) "**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.
- (b) "**Agreement**" means any agreement between Clarivate and Client under which Clarivate provides one or more of the Services to Client that incorporates this DPA. This DPA or other data processing terms incorporated into such Agreement by reference are, collectively, the "Agreement."
- (c) "**Authorized Affiliate**" means any of Client's Affiliate(s) which (a) is subject to the EU Data Protection Laws and (b) is permitted to use the Services pursuant to the Agreement between the Client and Clarivate but has not signed its own Order Form with Clarivate and is not a "Client" as defined under this DPA.
- (d) "**Client Personal Data**" means any personal data that Clarivate processes as a processor on behalf of Client via the Service, as more particularly described in this DPA. For the purposes of clarity, Client Personal Data does not include personal data for which Clarivate is a controller and processes in accordance with Clarivate's [Corporate Privacy Notice](#).
- (e) "**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" shall be construed accordingly.
- (f) "**Data Protection Laws**" means all data protection laws and regulations applicable to a party's processing of Client Personal Data under the Agreement, including, where applicable, EU Data Protection Law; the California Consumer Privacy Act ("CCPA"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); the Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018; the Privacy Act 1988 of Australia, as amended ("Australian Privacy Law"); and the UK Data Protection Law.
- (g) "**EU Data Protection Law**" means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii).
- (h) "**EU SCCs**" means the standard contractual clauses for processors as approved by the European Commission.
- (i) "**Europe**" means, for the purposes of this DPA, the European Union, the European Economic Area and/or their member states, and Switzerland.
- (j) "**Personal Data Breach**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Client Personal Data on systems managed or otherwise controlled by Clarivate.
- (k) "**Services**" means the relevant services identified in the Agreement.
- (l) "**SCCs**" means the EU SCCs and the UK Addendum.
- (m) "**Special Category of Personal Data**" means (a) genetic data (b) biometric data for the purpose of uniquely identifying a natural person; (c) data concerning health or a natural person's sex life or sexual orientation; (d) personal data revealing racial, ethnic, political or religious beliefs, or trade union membership and (e) personal data relating to criminal convictions and offenses.

**(n) "Sub-processor"** means any processor engaged by Clarivate or its Affiliates to assist in fulfilling its obligations with respect to providing the Service pursuant to the Agreement or this DPA. Sub-processors may include third parties or Affiliates of Clarivate but shall exclude Clarivate employees, contractors, or consultants.

**(o) "UK Addendum"** means the international data transfer addendum to the EU Commission standard contractual clauses as issued by the UK Information Commissioner's Office.

**(p) "UK Data Protection Law"** means any applicable current and future data protection, privacy and electronic marketing laws and regulations, including the UK Data Protection Act 2018, the GDPR as implemented into the laws of the United Kingdom ("UK GDPR") and the Privacy and Electronic Communications Regulations 2003.

**(q) "UK International Transfer"** means a transfer of personal data for which appropriate safeguards are required, from time, under UK Data Protection Law.

The terms "**appropriate safeguards**", "**controller**", "**data subject**", "**personal data**", "**processor**" and "**processing**" shall have the meaning given to them under applicable Data Protection Laws or if not defined thereunder, the GDPR, and "**process**", "**processes**" and "**processed**", with respect to any Client Personal Data, shall be interpreted accordingly.

## 2. Roles and Responsibilities

**(a) Parties' roles.** If applicable Data Protection Laws apply to either party's processing of Client Personal Data, the parties acknowledge and agree that (i) with regard to the processing of Client Personal Data, Client is the controller and Clarivate is a processor acting on behalf of Client, as further described in Appendix A (Details of Data Processing) of this DPA; and (ii) Client Personal Data shall be handled in accordance with applicable Data Protection Laws.

**(b) Purpose limitation.** Clarivate shall process Client Personal Data only in accordance with Client's documented lawful instructions and as necessary to comply with applicable law. The parties agree that this DPA and the Agreement sets out Client's complete and final instructions to Clarivate in relation to the processing of Client Personal Data, and processing outside the scope of these instructions (if any) shall be in writing between the parties ("Permitted Purposes").

**(c) Prohibited data.** Unless otherwise set forth in Appendix A of this DPA, Client will not provide (or cause to be provided) any Special Category of Personal Data to Clarivate for processing under the Agreement, and Clarivate will have no liability whatsoever for such data, whether in connection with a Personal Data Breach or otherwise.

**(d) Client compliance.** Client represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its processing of Client Personal Data and any processing instructions it issues to Clarivate; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for Clarivate to process Client Personal Data for the purposes described in the Agreement. Client shall have sole responsibility for the accuracy, quality, and legality of Client Personal Data and the means by which Client acquired Client Personal Data.

**(e) Lawfulness of Client's instructions.** Client will ensure that Clarivate's processing of the Client Personal Data in accordance with Client's instructions will not cause Clarivate to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws. Clarivate shall immediately notify Client in writing, unless prohibited from doing so under applicable Data Protection Laws, if it becomes aware or believes that any data processing instruction from Client violates the GDPR or any UK implementation of the GDPR.

## 3. Sub-processing

**(a) Authorized Sub-processors.** Client provides Clarivate with general written authorization to engage Sub-processors to process Client Personal Data on Client's behalf for the purposes of providing the Services. Clarivate will make a list of relevant Sub-processors available to Client **here** or by written request to [data.privacy@clarivate.com](mailto:data.privacy@clarivate.com). The list includes our Sub-processors, their respective jurisdictions of organisation and a description of their activities, together with publication of replacements or additions of Sub-processors and instructions on how Client may subscribe to receive prior notifications of such replacements and additions. Upon subscription, Clarivate shall inform Client of any intended changes concerning such addition or replacement of Sub-processors and if Client objects to the engagement of a new Sub-processor on reasonable grounds within ten (10) days upon such notice, Clarivate will use reasonable efforts to make a change in the Services or recommend a commercially reasonable change to avoid processing by such Sub-processor. In the event Clarivate is unable to make available such an alternative approach within a reasonable period of time, Client may terminate only the affected Services which cannot be provided without the use of the objected-to new sub-processor, without penalty or liability for either party, by providing written notice of

termination to Clarivate within thirty (30) days and Client shall be entitled to receive a refund of prepaid fees for the terminated Service on a pro-rated basis.

**(b) Sub-processor obligations.** Clarivate shall: (i) enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Client Personal Data as those in this DPA; and (ii) remain liable for the performance of such Sub-processor's compliance with the obligations under this DPA.

## 4. Security

**(a) Security Measures.** Clarivate shall implement and maintain appropriate technical and organizational security measures that are designed to protect Client Personal Data from Personal Data Breach and designed to preserve the security and confidentiality of Client Personal Data in accordance with Clarivate's security standards described in Appendix B ("Technical and Organizational Measures").

**(b) Confidentiality of processing.** Clarivate shall ensure that individuals authorized by Clarivate to process Client Personal Data shall be under an appropriate obligation of confidentiality.

**(c) Updates to Security Measures.** Client is responsible for reviewing the information made available by Clarivate relating to data security and making an independent determination as to whether the Service meets Client's requirements and legal obligations under Data Protection Laws. Client acknowledges that the Security Measures are subject to technical progress and development and that Clarivate may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service provided to Client.

**(d) Personal Data Breach response.** Upon becoming aware of a Personal Data Breach, Clarivate shall: (i) notify Client without undue delay, and where feasible, no later than 48 hours upon determining that a Personal Data Breach has occurred; (ii) provide timely information relating to the Personal Data Breach as it becomes known or as is reasonably requested by Client; and (iii) promptly take reasonable steps to contain and investigate any Personal Data Breach. Client agrees that an unsuccessful Personal Data breach will not be subject to this Section 4(d). An unsuccessful Personal Data Breach is one that results in no unauthorised access to Client Personal Data or any facilities or equipment of Clarivate storing Client Personal Data. Clarivate's notification of or response to a Personal Data Breach under this Section 4(d) shall not be construed as an acknowledgment by Clarivate of any fault or liability with respect to the Personal Data Breach.

## 5. Audits

**(a) Client's audit rights.** To the extent Clarivate holds a System and Organization Controls (SOC) 2 report, System and Organization Controls (SOC) 3 report or ISO 27001 certification conducted by independent third parties that cover the Services, Client agrees to exercise any right Client may have to conduct an audit or inspection under this DPA or under the SCCs if they apply, by instructing Clarivate in writing to provide a copy of its most current report or certification, which will be considered Clarivate's Confidential Information. If the SCCs apply, nothing in this Section modifies or affects any supervisory authority's or data subject's rights under the SCCs. In the event Clarivate fails to provide such report or certification, Client shall have the right, to conduct an audit, limited to once per year unless there has been a Personal Data Breach or an official complaint relating to our privacy and security practices.

**(b) Notification and scope.** Upon at least 30 days written notice by Client, Clarivate shall make available to Client all information necessary to demonstrate compliance with this DPA and as required by Data Protection Laws, allow for, and contribute to audits, including inspections by Client to assess compliance with this DPA. Before the commencement of any audit, Client and Clarivate shall mutually agree upon the scope, timing, and duration of the audit. Client shall reimburse Clarivate for any time expended by Clarivate or its third-party Sub-processors for any such audit. In the event an audit on our Sub-processors is requested, Client acknowledges that such audit may be subject to additional or different audit terms. All reimbursement rates shall be reasonable, taking into account the resources expended by Clarivate, or its third-party Sub-processors. Audits and inspections are subject to Clarivate's reasonable data protection policies, and do not extend to employee payroll, personnel records, or any portions of Clarivate's sites, books, documents, records, or other information that do not relate to the Client Personal Data or are otherwise commercially sensitive or legally privileged. The information obtained during an audit or inspection, and the results of such, will be considered Clarivate's Confidential Information.

## 6. International Transfers

**(a) Data center locations.** Subject to Sections 6(b) and 6(c) and except as otherwise agreed to in writing, Client acknowledges that Clarivate may transfer and process Client Personal Data to and in the United States and anywhere else in the world where

Clarivate, its Affiliates or its Sub-processors maintain data processing operations. As more particularly set forth below, Clarivate shall ensure that that a mechanism is in place to provide appropriate safeguards and enforcement of personal data protection in compliance with the requirements of Data Protection Laws and this DPA with respect to such transfers.

**(b) Australian transfers.** To the extent that Clarivate is a recipient of Client Personal Data protected by the Australian Privacy Law, the parties acknowledge and agree that Clarivate may transfer such Client Personal Data outside of Australia as permitted by the terms agreed upon by the parties and subject to Clarivate complying with this DPA and the Australian Privacy Law.

**(c) European Data transfers.** To the extent that Clarivate is a recipient of Client Personal Data protected by EU Data Protection Laws ("EU Data") in a country outside of Europe that is not recognized as providing an adequate level of protection for personal data (as described in applicable EU Data Protection Law), the parties agree to abide by and process EU Data in compliance with the EU SCCs in the form set out in Appendix C. For the purposes of the descriptions in the EU SCCs, Clarivate agrees that it is the "data importer" and Client is the "data exporter" (notwithstanding that Client may itself be an entity located outside Europe).

**(d) UK data transfers.** To the extent there is a UK International Transfer of Client Personal Data under and for the purposes of this DPA, the parties agree to abide by and process the relevant Client Personal Data in compliance with the UK Addendum in the form set out in Appendix D. For the purposes of the descriptions in the UK Addendum, Clarivate agrees that it is the "Importer" and Client is the "Exporter" (notwithstanding that Client may itself be an entity located outside of the UK).

**(e) Alternative transfer mechanism.** To the extent Clarivate adopts an alternative data export mechanism (including any new version of or successor to the SCCs) for the transfer of EU Data or UK Data not described in this DPA ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with applicable Data Protection Law and extends to the countries to which the applicable data is transferred). In addition, if and to the extent that a court of competent jurisdiction or supervisory authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer EU Data or UK Data (within the meaning of applicable Data Protection Law), Clarivate may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of such data.

## 7. Return or Deletion of Data

Upon termination or expiration of a Service and upon Client's written request and election made within 30 days after such termination or expiration, Clarivate shall (at Client's election) delete or return to Client all of Client Personal Data (including copies) in Clarivate's possession or control provided, however, that such return may result in additional charges to Client at Clarivate's then prevailing hourly rates. Such charges to be outlined in a separate quote and statement of work agreed to by both parties. This requirement shall not apply (i) to the extent Clarivate is required by applicable law to retain some or all of Client Personal Data; or (ii) to Client Personal Data Clarivate has archived on back-up systems, which Clarivate shall securely isolate and protect from any further processing until it is deleted in accordance with Clarivate's deletion policies.

## 8. Data Subject Rights and Cooperation

**(a) Data subject requests.** As part of the Service, Clarivate provides Client with several self-service features, that Client may use to retrieve, correct, delete, or restrict the use of Client Personal Data, which Client may use to assist it in connection with its obligations under the Data Protection Laws with respect to responding to requests from data subjects via Client's account at no additional cost. In addition, Clarivate shall, taking into account the nature of the processing, provide reasonable assistance to Client to the extent possible to enable Client to comply with its data protection obligations with respect to data subject rights under applicable Data Protection Laws. If any such request is made to Clarivate directly, Clarivate shall not without Client's prior authorization respond to such communication directly except as reasonably appropriate (for example, to direct the data subject to contact Client or to direct the data subject to a publicly available link with information on self-service functionality or to confirm the nature of the request and to which of our clients it is related) or if required by applicable law. If Clarivate is required to respond to such a request, Clarivate shall promptly notify Client and provide Client with a copy of the request unless Clarivate is legally prohibited from doing so.

**(b) Data protection impact assessment.** To the extent required under applicable Data Protection Laws, Clarivate shall (taking into account the nature of the processing and the information available to Clarivate) provide all reasonably requested information regarding the Service to enable Client to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws.

## 9. Jurisdiction-Specific Terms

To the extent Clarivate processes Client Personal Data originating from and protected by Data Protection Laws in one of the jurisdictions listed in Appendix E, then the terms specified in Appendix E with respect to the applicable jurisdiction(s) (“Jurisdiction-Specific Terms”) apply in addition to the terms of this DPA. In the event of any conflict or ambiguity between the Jurisdiction-Specific Terms and any other terms of this DPA, the applicable Jurisdiction-Specific Terms will take precedence, but only to the extent of the Jurisdiction-Specific Terms’ applicability to Clarivate.

## 10. Relationship with the Agreement

- (a) Term.** This DPA shall remain in effect for as long as Clarivate carries out Client Personal Data processing operations on behalf of Client or until termination of the Agreement (and all Client Personal Data has been returned or deleted in accordance with Section 7 above).
- (b) Precedence.** The parties agree that this DPA shall replace any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Service. In the event of any conflict or inconsistency between this DPA and the remainder of the Agreement with respect to the processing of Client Personal Data, the provisions of the following documents (in order of precedence) shall prevail: (i) SCCs; then (ii) this DPA; and then (iii) the remainder of the Agreement (which shall be interpreted in accordance with any order of precedence set forth therein).
- (c) Effects of changes.** Except for any changes made by this DPA, the Agreement remains unchanged and in full force and effect.
- (d) Third-party rights.** No one other than a party to this DPA, its successors and permitted assignees shall have any right to enforce any of its terms.
- (e) Governing law.** This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.
- (f) Authorized Affiliates.** The parties acknowledge and agree that, by executing the Agreement, Client enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Clarivate and each such Authorized Affiliate. Each Authorized Affiliate agrees to be bound by the obligations under this DPA. Client shall be responsible for coordinating all communication with Clarivate under this DPA and is entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates. Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Clarivate directly by itself, Client and each Authorized Affiliate agrees that (i) the Client who is the contracting party to the Agreement shall exercise any such rights or seek any such remedies on behalf of the Authorized Affiliate, (ii) the Client who is the contracting party to the Agreement shall exercise any such rights or seek any such remedies under this DPA in a combined manner for itself and all of its Authorized Affiliates together, and (iii) any reference to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and this DPA together. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement.

## Appendix A – Details of Data Processing

### Data Controller:

The Client and/or any Authorized Affiliates who qualify as controller under the terms of this DPA.

### Data Processor:

The Clarivate entity and/or its Affiliate(s) who process Client Personal Data under the terms of this DPA.

### Subject matter:

The subject matter of the data processing under this DPA is the Client Personal Data.

### Duration of processing:

Clarivate will process Client Personal Data as outlined in Section 7 and Section 10(a) of this DPA.

### Purpose and nature of processing:

The purpose and nature of the processing of the Client Personal Data shall include: (i) processing as necessary to provide the Services in accordance with the Agreement; (ii) to fulfil Clarivate’s contractual obligations under the Agreement and this DPA; and (iii) to comply with any other reasonable instructions provided by data controller (e.g., via email or support tickets) that are consistent with the terms of the Agreement and (iv) as set forth by such applicable Service below.

### Categories of data subjects:

Controller may submit Client Personal Data to the Services, the extent of which is determined and controlled by controller in its sole discretion, and which may include, but is not limited to Client Personal Data relating to the categories of data subjects set forth by Service below.

### Categories of personal data:

Controller may submit Client Personal Data to the Services consistent with the purposes for which the Services are provided, the extent of which, subject to any restrictions set forth herein or the Agreement, is determined and controlled by data controller in its sole discretion, and which may include, but is not limited to the categories of personal data set forth by Service below and in product documentation provided.

Service	Purpose and nature	Categories of data subjects	Categories of personal data
Converis	Hosting, implementation and/or technical support	<ul style="list-style-type: none"> <li>Employees, agents, advisors and contractors of controller</li> <li>Individuals authorized by controller to use the Services</li> <li>Members of the academic community such as peer reviewers, editors of participating journals</li> <li>Other data subjects as determined by controller</li> </ul>	<ul style="list-style-type: none"> <li>Name and other non-sensitive identifiers such as employee ID number, ResearcherID, username)</li> <li>Demographic information</li> <li>Business contact information</li> <li>Professional information</li> <li>Other categories of personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement</li> </ul>
Discovery, Research and Library Workflow Solutions: 360 Core 360 LINK 360 MARC Updates 360 Resource Manager 360 Search	Hosting, implementation and/or technical support	<ul style="list-style-type: none"> <li>library patrons, library staff, faculty, students, administrators, employees, visitors and alumni</li> </ul>	<ul style="list-style-type: none"> <li><u>Basic user and patron information, including</u> <ul style="list-style-type: none"> <li><u>First and last names</u></li> <li><u>Postal addresses</u></li> <li><u>Email addresses</u></li> <li><u>Telephone numbers and other contact information</u></li> <li><u>Institutional identification numbers</u></li> <li><u>Department and Role</u></li> </ul> </li> <li><u>Basic staff and staff contact information</u></li> <li><u>Staff related usage information, including records of staff operations and activity</u></li> </ul>

<p>Intota™ Assessment Pivot/Pivot-RP RefWorks Summon Ulrichsweb Ulrich's™ Serials Analysis System Intota™</p>			<ul style="list-style-type: none"> <li>• <a href="#">Research activity</a></li> <li>• <a href="#">General usage information, including connection data (e.g., IP addresses)</a></li> <li>• <a href="#">Suppliers/vendors information</a></li> </ul>
<p>First to File</p>	<p>User account pre-registration; hosting; implementation and/or technical support; and professional services as applicable</p>	<ul style="list-style-type: none"> <li>• Employees, agents, advisors, freelancers of controller (who are natural persons)</li> <li>• Individuals authorized by controller to use the Services</li> <li>• Prospects, customers, business partners and vendors of controller (who are natural persons)</li> <li>• Employees or contact persons of controller's prospects, customers, business partners and vendors</li> <li>• Other data subjects as determined by controller including inventors, patent applicants and assignees, trademark owners, attorneys</li> </ul>	<ul style="list-style-type: none"> <li>• Name and other non-sensitive identifiers such as signatures</li> <li>• Business Contact information</li> <li>• Demographic information</li> <li>• Professional information</li> <li>• Other categories of personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement</li> </ul>
<p>Integrated Library Systems: Millennium Polaris Sierra Vega Virtua and associated modules</p>	<p>Hosting (unless hosted by the controller or an authorized third-party hosting provider), implementation and/or technical support</p>	<ul style="list-style-type: none"> <li>• Employees, agents, advisors, freelancers of controller (who are natural persons)</li> <li>• Individuals authorized by controller to use the Services, including library patrons</li> </ul>	<ul style="list-style-type: none"> <li>• Library patron data such as library card number or other identifying number, which may include an image of Data Subject's library card, age or date of birth, contact information, proof of residency, which can include copies of a government-issued identification card or other documents that data subject provided to Client</li> <li>• Information about use of the Services; for library patrons, this may include, for example, use of library resources (including locations or branches visited, history of materials requested, held, checked out, or accessed)</li> <li>• Interactions with library staff</li> <li>• Use of other library services; information provided to facilitate any payments; and any late fees or fines</li> <li>• Name and other non-sensitive identifiers such as employee ID number and username</li> <li>• Business Contact information</li> <li>• Demographic information</li> <li>• Professional information</li> <li>• Other categories of personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement</li> </ul>
<p>IP management systems: FoundationIP IPfolio Ipendo Inprotech Memotech Patrawin The IP Management System Unycom</p>	<p>Hosting (unless hosted by the controller or an authorized third-party hosting provider such as Salesforce), implementation and/or technical support</p>	<ul style="list-style-type: none"> <li>• Employees, agents, advisors, freelancers of controller (who are natural persons)</li> <li>• Individuals authorized by controller to use the Services</li> <li>• Prospects, customers, business partners and vendors of controller (who are natural persons)</li> <li>• Employees or contact persons of controller's prospects, customers, business partners and vendors</li> </ul>	<ul style="list-style-type: none"> <li>• Name and other non-sensitive identifiers such as employee ID number and username</li> <li>• Business Contact information</li> <li>• Demographic information</li> <li>• Professional information</li> <li>• Other categories of personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement</li> </ul>

		<ul style="list-style-type: none"> <li>• Other data subjects as determined by controller including inventors, patent applicants and assignees, trademark owners, attorneys</li> </ul>	
<b>IP Professional Services</b>	Provision of IP-related professional services including without limitation renewals, docketing and filing services	<ul style="list-style-type: none"> <li>• Employees, agents, advisors, freelancers of controller (who are natural persons)</li> <li>• Individuals authorized by controller to use the Services</li> <li>• Prospects, customers, business partners and vendors of controller (who are natural persons)</li> <li>• Employees or contact persons of controller's prospects, customers, business partners and vendors</li> <li>• Other data subjects as determined by controller including inventors, patent applicants and assignees, trademark owners, attorneys</li> </ul>	<ul style="list-style-type: none"> <li>• Name and other non-sensitive identifiers such as employee ID number and username</li> <li>• Business Contact information</li> <li>• Demographic information</li> <li>• Professional information</li> <li>• Other categories of personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement</li> </ul>
<b>Market research - Contractually required safety and quality reporting as part of a market research engagement</b>	Reporting to Client or Market Authorization Holder of safety and quality events as set forth in the Agreement	Market research participants	<ul style="list-style-type: none"> <li>• Name</li> <li>• Demographic information</li> <li>• Professional information</li> <li>• Contact information</li> <li>• Information required to process honoraria</li> </ul>
<b>Market research - List-based recruiting for primary market research projects</b>	Handling of list provided by Client for the purposes of recruiting specific individuals for primary market research	Potential market research participants	<ul style="list-style-type: none"> <li>• Name</li> <li>• Demographic information</li> <li>• Contact information</li> <li>• Professional information</li> <li>• Information required to process honoraria</li> </ul>
<b>My Organization (InCites Benchmarking and Analytics Module)</b>	Enabling Client to upload, analyze and manage its researchers' database on the Clarivate's My Organization modules of InCites	<ul style="list-style-type: none"> <li>• Employees, agents, advisors and contractors of controller (who are natural persons)</li> <li>• Individuals authorized by controller to use the Services</li> <li>• Other data subjects as determined by controller</li> </ul>	<ul style="list-style-type: none"> <li>• Name and other non-sensitive identifiers such as employee ID number, ResearcherID, username</li> <li>• Demographic information</li> <li>• Business contact information</li> <li>• Professional information</li> <li>• Other categories personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement</li> </ul>
<b>Cloud-based library management, discovery, research, reading list and mobile/web app (Ex Libris SaaS services):</b>  <b>Alma</b> <b>Esploro</b> <b>CampusM</b> <b>Leganto</b>	Hosting, implementation, technical support and/or other related services	Library patrons, library staff, faculty, students, administrators, employees, researchers, visitors and alumni	<ul style="list-style-type: none"> <li>• <u>Basic user and patron information, including</u> <ul style="list-style-type: none"> <li>○ <u>First and last names</u></li> <li>○ <u>Postal addresses</u></li> <li>○ <u>Email addresses</u></li> <li>○ <u>Telephone numbers and other contact information</u></li> <li>○ <u>Institutional identification numbers</u></li> </ul> </li> <li>• <u>Library/catalogue related user and patron information, including</u> <ul style="list-style-type: none"> <li>○ <u>Library activity, loans and fines information</u></li> </ul> </li> <li>• <u>Basic staff information, including contact information</u></li> <li>• <u>Staff related usage information, including records of staff operations and activity</u></li> <li>• <u>Research activity</u></li> </ul>

<b>Primo SaaS/Primo VE</b>  <b>Rapido</b>			<ul style="list-style-type: none"> <li>• <u>General usage information, including connection data (e.g., IP addresses)</u></li> <li>• <u>Suppliers/vendors information</u></li> <li>• <u>Mobile Platform information, if applicable</u> <ul style="list-style-type: none"> <li>○ <u>Device information (e.g., identifier and platform)</u></li> <li>○ <u>Attendance and location data, if applicable</u></li> </ul> </li> </ul>
<b>Software Support and Maintenance Services for Locally Installed Ex Libris Software, including:</b>  <b>Aleph Local</b>  <b>Primo Local</b>  <b>Rosetta Local</b>  <b>Voyager Local</b>  <b>SFX</b>	Performance of Support and Maintenance by remote access to locally installed versions of listed products	Categories of Data Subjects as selected by Client and stored on its locally installed systems to which Clarivate may have temporary access	<ul style="list-style-type: none"> <li>• Personal Data types stored by Client on the local systems running the Programs to which Clarivate will have access in connection with providing the Software Maintenance and Support Services and/or provided by Client to Clarivate in the course of providing the Software Maintenance and Support Services</li> <li>• Processing is very limited and involves primarily incidental access to Personal Data during active and temporary remote accessing of systems to resolve a support service call</li> </ul>
<b>Web of Science Reviewer Recognition;</b>  <b>Web of Science Author Connect</b>  <b>Web of Science Reviewer Locator</b>	Only for handling lists (provided by Client) of individuals who will be invited to sign up to the applicable Service	Members of the academic community such as researchers and peer reviewers	<ul style="list-style-type: none"> <li>• Name and other non-sensitive identifiers such as ResearcherID</li> <li>• Demographic information</li> <li>• Business contact information</li> <li>• Professional information</li> <li>• Other information associated with the data subjects' peer review activities</li> </ul>
<b>ScholarOne</b>	Hosting, technical support and associated services	<ul style="list-style-type: none"> <li>• Employees, agents, advisors and contractors of controller (who are natural persons)</li> <li>• Members of the academic community such as publication authors and peer reviewers</li> <li>• Other data subjects as determined by controller</li> </ul>	<ul style="list-style-type: none"> <li>• Name and other non-sensitive identifiers such as employee ID number, ResearcherID, username</li> <li>• Demographic information</li> <li>• Business contact information</li> <li>• Professional information</li> <li>• Other categories personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement</li> </ul>

### Special Categories of Personal Data (as defined by the GDPR) or Sensitive Data:

Clarivate does not want to, nor does it intentionally, collect or process any Special Categories of Personal Data in connection with the provision of the Service except for health-related details that are processed due to contractually required reportable safety and/or quality events as part of a market research engagement.

### Processing Operations:

Client Personal Data will be processed in accordance with the Agreement (including this DPA and any Statements of Work or Order Forms) and as necessary to provide, maintain and improve the Services provided to Client pursuant to the Agreement and/or as compelled by applicable law, and may be subject to the following processing operations:

Any operation or set of operations, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

### Frequency of Personal Data Transfer:

Client Personal Data will be transferred at the outset and throughout the Term where necessary.

**Period of Retention:**

Data will be retained during the Term and as outlined in Section 7 of the DPA.

The descriptions above also apply to Clarivate's transfers to Sub-processors.

## Appendix B – Technical and Organizational Measures

The technical and organizational measures applicable to the Service are described here (as updated from time to time in accordance with Section 4(c) of this DPA).

### **Information Security Program**

Clarivate has a well-defined Information Security Program that encompasses relevant aspects of technical and organizational measures aligned with well-known industry standards for Information Security to protect the confidentiality, integrity and availability of information assets

### **Personnel**

All our staff are subject to our code of conduct encompassing our company's values and mission. They are made aware of their responsibilities, our policies and standards and receive regular guidance and support from our Information Security team.

In accordance with relevant laws and regulations, adequate background verification checks are performed while recruiting an individual as permanent staff to reduce the possibility of threat to critical information assets.

We conduct mandatory information security training on an ongoing basis and provide supplemental training to specific target groups and individuals as required. Our staff are bound by obligations of confidentiality and understand the consequences for failing to adhere to our policies and their responsibilities.

An employee exit process is followed at Clarivate which involves revocation of system permissions/access rights and return of company assets in a timely manner.

### **Encryption of personal data**

Measures, including encryption, are used to ensure that personal data cannot be read, copied, modified or deleted without authorization during electronic transmission or transport, and that the target entities for any transfer of personal data by means of data transmission facilities can be established and verified.

### **User Access management**

Clarivate has a well-defined process for granting access to information assets. We have established measures to prevent unauthorized persons from using data processing equipment including access management, log records and password protections.

User privileges to data processing equipment are granted to restrict access to such personal data in accordance with their roles and responsibilities to protect against unauthorized access and disclosure. Clarivate password policy is defined across the board on all information assets, with a minimum length, complexity, password expiry, history and account lockout requirements in case of failed attempts.

### **Infrastructure security**

Our services are offered through public and private networks. Communications are protected against eavesdropping by secure channels, and encryption. Clarivate has secured its perimeter with Intrusion Prevention Systems (IPS), firewall and/or security groups for AWS to manage and restrict network access, and VLANS in our data center.

There are tiered controls, including the use of network segmentation, designed to ensure the appropriate level of protection to systems and data.

### **Malware protection**

In line with our policies, Clarivate owned and supported operating systems which are hosted in our data centers or deployed in the cloud are protected with a next generation antivirus solution.

### **Patch management**

We gather and review security threat intelligence from our internal vulnerability management tools, vendors and other third-party security organizations. Our patch management standard provides appropriate patching practices to our technology teams.

Our security patching starts with evaluation and definition of the severity of the patch. Priority certification and full QA testing is employed to validate the stability and availability of the systems post-patching. At times, additional security controls may be implemented to provide mitigation against known threats.

### **Security monitoring**

Clarivate has a dedicated Network & Security Operations Center (NOC/SOC) that provides 24x7 logging and monitoring for logical network access to customer data and information asset usage. Security logs are sent to our SOC (Security Operation Center) for the purpose of real-time awareness, event correlation and incident response. Logging of data entry also takes place, to ensure that it is possible to check and ascertain whether personal data has been entered into, altered or removed from personal data processing systems and if so, by whom.

### **Security and Privacy Incident response**

An incident response process is in place to address incidents as they are identified. Incidents are managed by a dedicated incident response team which follows a documented procedure for mitigation and communications.

Clarivate's Incident Response process requires incidents to be effectively reported, investigated, and monitored to ensure that corrective action is taken to control and remediate security incidents in a timely manner.

### **Operations Security**

Changes to operating information systems environment which includes changes to servers, network equipment and software are subject to formal change management process.

Backup copies of information and software are safely maintained for the purpose of data recovery in case of events such as system crash or accidental deletion of information.

### **Capacity management and monitoring**

Monitoring of systems, services and operations are implemented to maintain the health of our operating environments. Management tools are implemented to monitor and maintain an appropriately scaled environment.

### **Vulnerability scanning**

Clarivate has implemented a multi-tiered security vulnerability management program that includes security checks and automated or manual security reviews, application and infrastructure vulnerability assessment scans. Measures are in place to assess, validate, prioritize, and remediate identified issues.

Internet-facing sites on our global network are periodically scanned as a practice in our program focused on vulnerability management.

### **Risk Management**

Our product and technology teams engage information security subject matter experts regularly to provide risk assessments services. Architecture reviews, vulnerability scans, application security testing and technical compliance reviews are several of the services performed during risk assessment activities.

Following risk assessment activities our Information Security Risk Management team consults with product and technology teams to develop remediation plans and roadmaps to address gaps in compliance, or areas of identified risk.

Additionally, our IT Governance, Risk and Compliance team performs audits against policies, standards and regulatory requirements, and registers findings for review and remediation initiatives within the business.

### **Physical security and third-party vendor management**

All strategic datacenters, including cloud service providers hosting Clarivate products, are deployed and managed to the physical security industry standards that Clarivate has adopted. Our guidelines include requirements for physical security, building maintenance, fire suppression, air conditioning, UPS with generator back-up, and access to diverse power and communications. Clarivate reviews third party datacenters assurance reports as part of our Vendor Risk Management program.

A variety of secure methods are used to control access to our facilities to ensure that access is only gained in a controlled way on an operational needs basis. Depending on the sensitivity of the facility, these methods may include some or all of the

following: the use of alarm device or security service outside service times, Division of premises into different security zones, security staff, ID cards, electronic access control incorporating proximity card readers, physical locks and pin numbers.

# Appendix C - EU Standard Contractual Clauses (Processor)

## Controller to Processor

### SECTION I

#### Clause 1

##### Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 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) for the transfer of data to a third country.
- (b) The Parties:
- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')
- have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### Clause 2

##### Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

#### Clause 3

##### Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - (iii) Clause 9 – Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 – Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 – Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

#### **Clause 4**

##### **Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### **Clause 5**

##### **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### **Clause 6**

##### **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### **Clause 7 – Optional**

*[Intentionally omitted.]*

## **SECTION II – OBLIGATIONS OF THE PARTIES**

#### **Clause 8**

##### **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

##### **8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

##### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

##### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

##### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

## 8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

## 8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

## 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### **8.9 Documentation and compliance**

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

## **Clause 9**

### **Use of sub-processors**

- (a) **GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance wherever commercially reasonable to do so, but no less than 5 days in advance in all instances, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### **Clause 10**

##### **Data subject rights**

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### **Clause 11**

##### **Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### **Clause 12**

##### **Liability**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### **Clause 13**

#### **Supervision**

- (a) Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

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) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States 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, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## **SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

### **Clause 14**

#### **Local laws and practices affecting compliance with the Clauses**

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of

- processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
- (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
  - (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
  - (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
  - (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **Clause 15**

### **Obligations of the data importer in case of access by public authorities**

#### **15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

#### **15.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

### **SECTION IV – FINAL PROVISIONS**

#### **Clause 16**

##### **Non-compliance with the Clauses and termination**

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### **Clause 17**

##### **Governing law**

In the event that the governing law of the Agreement (as defined in the DPA) is that of an EU Member State, these Clauses shall be governed by the law of such EU Member State, provided such law allows for third-party beneficiary rights. If such law does not allow for third-party beneficiary rights, or if the governing law of the Agreement is not that of an EU Member State, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

#### **Clause 18**

##### **Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of the EU Member State set forth in Clause 17.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

## ANNEX 1 TO THE EU STANDARD CONTRACTUAL CLAUSES

### A. LIST OF PARTIES

#### **Data exporter:**

The Client and/or Authorized Affiliates who transfer the Client Personal Data under the terms of Data Processing Addendum ("DPA") to which these Clauses are appended.

#### **Data importer:**

The Clarivate entity, acting as data importer on behalf of itself or its Affiliates where applicable, who agrees to receive from the Data Exporter Client Personal Data under the terms of DPA to which these Clauses are appended.

### B. DESCRIPTION OF THE TRANSFER

Please see the details set forth in Appendix A to the DPA to which these Clauses are appended.

### C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority will be the supervisory authority of the data exporter as required by Clause 13.

## ANNEX 2 TO THE EU STANDARD CONTRACTUAL CLAUSES

### **TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

As set forth in Appendix B of the DPA.

## ANNEX 3 TO EU STANDARD CONTRACTUAL CLAUSES

The parties acknowledge that Clause 2(a) of the Clauses permits them to include additional business-related terms provided they do not contradict, directly or indirectly, the Clauses or prejudice the fundamental rights or freedoms of data subjects.

Accordingly, this Annex sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Annex, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

### **Clauses 3 and 8.6(d): Disclosure of these Clauses**

Data exporter agrees that these Clauses constitute data importer's Confidential Information (as that term is defined in the Agreement) and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 3 or a supervisory authority pursuant to Clause 8.6(d).

### **Clause 8.1(a) and Clause 8.1(b): Suspension of data transfers and termination**

1. The parties acknowledge that for the purposes of Clause 8.1(a), data importer may process the personal data only on behalf of the data exporter and in compliance with its documented instructions as set out in the DPA and that pursuant to the DPA, these instructions shall be the data exporter's complete and final instructions and processing outside the scope of such instructions (if any) shall be in writing between the parties.
2. The parties acknowledge that if data importer cannot provide compliance in accordance with Clause 8.1(a) and/or Clause 8.1(b), the data importer agrees to promptly inform the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the affected parts of the Service in accordance with the terms of the Agreement.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate the affected parts of the Service, it shall first provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").
4. In addition, the data exporter and data importer shall reasonably cooperate with each other during the Cure Period to agree what additional safeguards or other measures, if any, may be reasonably required to ensure the data importer's compliance with the Clauses and applicable data protection law.
5. If, after the Cure Period, the data importer has not or cannot cure the non-compliance in accordance with the paragraphs 3 and 4 above, then the data exporter may suspend and/or terminate the affected part of the Service in accordance with the provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by the data exporter prior to suspension or termination).

### **Clause 8.9: Audit**

Data exporter acknowledges and agrees that it exercises its audit right under Clause 8.9 by instructing data importer to comply with the audit measures described in Section 5 (Audits) of the DPA.

### **Clause 9(c): Disclosure of subprocessor agreements**

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.
2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessor agreement to data exporter.

**Clause 12: Liability**

To the extent permissible, any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event, shall any party limit its liability with respect to any data subject rights under these Clauses.

## Appendix D - UK Addendum

In accordance with applicable data protection law, including the UK GDPR, Clarivate (hereinafter the "Importer") and Client (hereinafter the "Exporter") each a "party"; together "the parties", HAVE AGREED on the following Addendum in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Exporter to the Importer of the personal data specified in Annex 1.

### Part 1: Tables

Table 1: Parties

<b>Start date</b>	The date signed by both parties on the Agreement.	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	As described in the Agreement.	As described in the Agreement.
<b>Key Contact</b>	As described in Annex 1 of the attached EU SCCs.	As described in Annex 1 of the attached EU SCCs.
<b>Signature (if required for the purposes of Section 2)</b>	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses

<b>Addendum EU SCCs</b>	<p><input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date: Effective as of the date signed by both parties below (Module 2: standard contractual clauses for the transfer of personal data to third countries – controller to processor)</p>
-------------------------	---

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Please see Annex I of the attached EU SCCs.
Annex 1B: Description of Transfer: Please see Annex I of the attached EU SCCs.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Please see Annex 2 of the attached EU SCCs.
Annex III: List of Sub processors (Modules 2 and 3 only): This Annex III is not applicable because Clause 9(a), Option 1 (specific authorisation of sub processors) of the attached Addendum EU SCCs was not selected.

Table 4: Ending this Addendum when the Approved Addendum Changes

<b>Ending this Addendum when the Approved Addendum changes</b>	<p>Which Parties may end this Addendum as set out in Section 19:</p> <p><input type="checkbox"/> Importer</p> <p><input type="checkbox"/> Exporter</p> <p><input checked="" type="checkbox"/> neither Party</p>
--	---

## Part 2: Mandatory Clauses

### Entering into this Addendum

- Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this Addendum

- Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

<b>Addendum</b>	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
<b>Addendum EU SCCs</b>	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.

<b>Appendix Information</b>	As set out in Table 3.
<b>Appropriate Safeguards</b>	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
<b>Approved Addendum</b>	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
<b>Approved EU SCCs</b>	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
<b>ICO</b>	The Information Commissioner.
<b>Restricted Transfer</b>	A transfer which is covered by Chapter V of the UK GDPR.
<b>UK</b>	The United Kingdom of Great Britain and Northern Ireland.
<b>UK Data Protection Laws</b>	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
<b>UK GDPR</b>	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

#### Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting

terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

#### Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
  - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
  - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
  - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
  - a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
  - b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
  - c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
  - d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
  - e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
  - f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
  - g. References to Regulation (EU) 2018/1725 are removed;
  - h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
  - i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";
  - j. Clause 13(a) and Part C of Annex I are not used;
  - k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
  - l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;"
  - m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";
  - n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and
  - o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

#### Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:
  - a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
  - b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
  - a. its direct costs of performing its obligations under the Addendum; and/or
  - b. its risk under the Addendum,and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.
20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

## Appendix E - Jurisdiction-Specific Terms

### Europe and UK:

**(a) Objection to Sub-processors.** Client may object in writing to Clarivate's appointment of a new Sub-processor within ten (10) calendar days of receiving notice in accordance with Section 3(a) of DPA, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Clarivate will, at its sole discretion, either not appoint such Sub-processor, or permit Client to suspend or terminate the affected Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Client prior to suspension or termination).

**(b) Government data access requests.** As a matter of general practice, Clarivate does not voluntarily provide government agencies or authorities (including law enforcement) Client Personal Data. If Clarivate receives a compulsory request (whether through a subpoena, court order, search warrant, or other valid legal process) from any government agency or authority (including law enforcement) for access to Client Personal Data belonging to a data subject whose primary contact information indicates the data subject is located in Europe or the UK, Clarivate shall: (i) inform the government agency that Clarivate is a processor of the data; (ii) attempt to redirect the agency to request the data directly from Client; and (iii) notify Client via email sent to Client's primary contact email address of the request to allow Client to seek a protective order or other appropriate remedy. As part of this effort, Clarivate may provide Client's primary and billing contact information to the relevant authority. Clarivate shall not be required to comply with this paragraph (b) if it is legally prohibited from doing so, or it has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual, public safety, or to Clarivate.

### California:

**(a) Definitions.** Except as described otherwise, the definitions of: "controller" includes "Business"; "processor" includes "Service Provider"; "data subject" includes "Consumer"; "personal data" includes "Personal Information"; in each case as defined under CCPA. For this "California" section of Annex D only, "Permitted Purposes" shall include processing Client Personal Data only for the purposes described in this DPA and in accordance with Client's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, as otherwise agreed in writing, including, without limitation, in the Agreement, or as otherwise may be permitted for "service providers" under the CCPA.

**(b) Consumer's rights.** Clarivate's obligations regarding data subject requests, as described in Section 8 (Data Subject Rights and Cooperation) of this DPA, apply to Consumer's rights under the CCPA.

**(c) Permitted purpose.** Notwithstanding any use restriction contained elsewhere in this DPA, Clarivate shall process Client Personal Data only to perform the Services, for the Permitted Purposes and/or in accordance with Client's documented lawful instructions, except where otherwise required by applicable law. Clarivate may de-identify or aggregate Client Personal Data as part of performing the Service specified in this DPA and the Agreement.

**(d) Sub-processors.** Where Sub-processors process the personal data of Client contacts, Clarivate takes steps to ensure that such Sub-processors are Service Providers under the CCPA with whom Clarivate has entered into a written contract that includes terms substantially similar to this DPA or are otherwise exempt from the CCPA's definition of "sale". Clarivate conducts appropriate due diligence on its Sub-processors. Where Sub-processors process the personal data of Client contacts, Clarivate takes steps to ensure that such Sub-processors are Service Providers under the CCPA with whom Clarivate has entered into a written contract that includes terms substantially similar to this DPA or are otherwise exempt from the CCPA's definition of "sale". Clarivate conducts appropriate due diligence on its Sub-processors.

### Canada:

**(a) Sub-processors.** Clarivate takes steps to ensure that Clarivate's Sub-processors, as described in Section 3 (Sub-processing) of the DPA, are third parties under PIPEDA, with whom Clarivate has entered into a written contract that includes terms substantially similar to this DPA. Clarivate conducts appropriate due diligence on its Sub-processors.

**(b) Security.** Clarivate will implement technical and organizational measures as set forth in Section 4 (Security) of the DPA.

Last Update: July 2022 (Version 2)