Data Processing Addendum

This Data Processing Addendum (including its Appendices, the "**DPA**") is incorporated into the Agreement (as defined below) 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").

This DPA sets out the terms, requirements, and conditions on which Clarivate will process Client Personal Data (as defined below) when providing its Services under the Agreement. Clarivate reserves the right to update this DPA from time to time. In the event of any such updates, Clarivate shall notify Client accordingly. In case of any conflict or inconsistency between this DPA, the Agreement and any other applicable agreements between Clarivate and Client, the terms of this DPA shall prevail.

Capitalized terms used but not defined in this DPA shall have the meanings set forth in the Agreement.

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, and that incorporates this DPA.

c) **"Client Personal Data"** means any personal data that Clarivate processes in the context of the Services provided to Client under the Agreement.

d) **"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.

e) **"Data Protection Laws"** means all data protection and privacy laws and regulations which apply to a party's processing of Client Personal Data under the Agreement, including, but not limited to, the EU General Data Protection Regulation ("**GDPR**"); the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("**CCPA**"); the Children's Online Privacy Protection Act ("**COPPA**"), the Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"); the Brazilian General Data Protection Law ("**LGPD**"); the Privacy Act 1988 of Australia ("**Australian Privacy Law**"); the Swiss Federal Act on Data Protection ("**FADP**"); and the GDPR as adopted by the UK ("**UK GDPR**"), each as amended from time to time.

f) **"EU SCCs"** means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR adopted by the European Commission, in particular Module One (controller to controller) (if applicable) and Module Two (controller to processor), as updated from time to time.

g) **"Europe"** means, for the purposes of this DPA, the European Union and the European Economic Area and/or their member states.

h) **"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.

i) **"Services"** means the relevant services identified in the Agreement.

j) **"Special Category of Personal Data"** means personal data (i) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, and (ii) relating to criminal convictions and offenses.

k) **"Sub-processor"** means any third parties or Affiliates of Clarivate, as applicable, engaged by Clarivate to assist in fulfilling Clarivate's obligations with respect to providing the Service pursuant to the Agreement.

l) **"UK Addendum"** means the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0, in force 21 March 2022)" as issued by the UK Information Commissioner's Office ("**UK ICO**").

The terms "**appropriate safeguards**", "**controller**", "**sell**", "**share**", "**data subject**", "**personal information**", "**personal data**", "**processor**" and "**processing**", including any variations of "processing", shall have the meaning given to them under Data Protection Laws. To the extent that these terms have terms with equal or similar meaning under Data Protection Laws, these equal or similar terms shall apply.

2. Roles and Responsibilities

(a) **Parties' roles**. If Data Protection Laws apply to either party's processing of Client Personal Data, the parties acknowledge and agree that with regards to the processing of Client Personal Data, Client is the controller and Clarivate is a processor, as further described in Appendix A ("**Details of Data Processing**") of this DPA. In deviation from this general allocation of the parties' role, Clarivate may process Client Personal Data as a separate independent controller to the extent that it processes Client Personal Data for statistical analysis for operational purposes such as billing and account management, financial reporting, business modelling and internal reporting, as further detailed in Clarivate's privacy policy, available at https://clarivate.com/legal/privacy-statement/.

(b) **Purpose limitation**. Clarivate shall process Client Personal Data in accordance with Client's documented lawful instructions and as necessary to comply with applicable laws; in the latter case, to the extent this is not prohibited under the relevant laws on important grounds of public interest, Clarivate shall inform Client of the relevant legal requirements. The parties agree that this DPA and the Agreement set 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 agreed 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, and Clarivate will have no liability whatsoever for its processing of such data, whether in connection with a Personal Data Breach or otherwise. This shall also apply to other categories of Personal Data prohibited by the Agreement or Data Protection Laws.

(d) **Client compliance**. Client represents and warrants that it has complied, and will continue to comply, with all Data Protection Laws, in respect of its processing of Client Personal Data and any processing instructions it issues to Clarivate. Client shall have sole responsibility for the accuracy, quality, and legality of Client Personal Data and the means by which Client collected Client Personal Data. Client shall hold Clarivate harmless for any non-compliance with Data Protection Laws to the extent that Clarivate acts as a processor in accordance with Client's instructions and the terms of this DPA and the Agreement.

(e) **Lawfulness of Client's instructions**. Client shall 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. If Clarivate becomes aware that any data processing instruction from Client violates applicable laws, including Data Protection Laws, Clarivate may cease processing the relevant Client Personal Data. In such case, Clarivate shall notify Client in writing within a reasonable timeframe. If Client does not adapt its instruction causing the violation of applicable laws, Clarivate may immediately terminate the Agreement and this DPA.

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. Client may access the list of Sub-processors via Clarivate's Privacy centre (see under "Transparency and choice") or request it directly from Clarivate by reaching out to **data.privacy@clarivate.com**. Further, Client may subscribe to receive notifications of any intended replacements and additions of its Sub-processors via the form included in the list of Sub-processors. 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-rata 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 a similar 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 (where required by Data Protection Laws).

4. Security

(a) Security measures. Clarivate shall implement and maintain appropriate technical and organizational security measures ensuring a level of security appropriate to the risks for the 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 as soon as reasonably practical, and, in any event, 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. 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. Upon at least sixty (60) days written notice by Client, Clarivate shall make available to Client all information which is reasonably necessary to demonstrate compliance with this DPA, and shall allow for, and contribute to audits (where reasonable to do so), including inspections by Client to assess compliance with this DPA to be conducted at the Client's sole cost. 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 its audit right by instructing Clarivate in writing to provide a copy of its most current report or certification, which will be considered Clarivate's Confidential Information. In the event Clarivate fails to provide such report or certification, Client, including by a mandated auditor, shall have the right to conduct an own audit at its own expenses, limited to once per year unless Clarivate has been subject to a Personal Data Breach or Clarivate has been subject to an official complaint relating to its privacy and security practices.

(b) Scope and terms applicable to the Client's audit. The auditor mandated by Client shall be no competitor of Clarivate and shall be subject to a non-disclosure agreement, satisfactory to Clarivate, obligating the auditor to maintain the confidentiality of Clarivate's Confidential Information and all audit findings. 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's costs for any time expended by Clarivate for any such audit. In the event an audit on Clarivate's Sub-processors is requested, Client acknowledges that such audit may be subject to additional or different audit terms. All reimbursement rates and costs shall be subject to Clarivate's hourly rates, 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 and information security policies. The scope of the audit shall be limited to Clarivate's information systems, or policies and procedures applicable to the protection of Client Personal Data. Client agrees to not review Clarivate's raw data, private, sensitive, confidential, or proprietary business information including 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. Client shall not copy Clarivate's security information or any materials or remove same from Clarivate's premises or systems.

Client shall provide Clarivate with a copy of the audit findings, at no cost to Clarivate. Upon completion of an audit, Client shall immediately notify Clarivate, in detail, of any claims that Clarivate is non-compliant with its security,

confidentiality, or data protection obligations under this DPA discovered during the audit, if applicable. The information obtained during an audit or inspection, and the results of such, will be considered Clarivate's Confidential Information.

6. International Data Transfers

(a) **Data transfers from Clarivate to third parties**. Subject to the terms in Section 3 and this Section 6, Clarivate may transfer Client Personal Data to data recipients based in third countries within the meaning of the Data Protection Laws subject to ensuring compliance with the provisions for cross-border data transfers under the Data Protection Laws.

(b) **GDPR data transfers**. To the extent that Clarivate is based outside the EU/EEA and receives Client Personal Data protected under the GDPR, but no adequacy decision within the meaning of Article 45(3) GDPR applies to the transfer, the parties agree to enter into the EU SCCs by entering into this DPA. Therefore, the EU SCCs shall be deemed incorporated to this DPA, whereas Clarivate shall be the "data importer" and Client the "data exporter". In particular, the parties agree that (i) Clause 7 of the EU SCCs shall not apply, (ii) for Module Two: Option 2 (general 4uthorization) in Clause 9(a) shall apply and the time period shall be at least ten (10) days, (iii) there shall be no dispute resolution body (Clause 11), (iv) Option 2 under Clause 17 shall apply and the law of the Member State as identified under the Agreement shall apply and if no Member State law is agreed, the law of Ireland, and (v) the choice of forum under Clause 18 shall be as agreed in the Agreement and if no courts of a Member State are agreed, the courts of Ireland shall be agreed. The required information under Annex 1 of the EU SCCs is set out in Appendix A of this DPA, whereas the competent supervisory authority shall be the authority competent for the data exporter as identified under Clause 13 of the EU SCCs. The required information under Annex 2 of the EU SCCs is set out in Appendix B of this DPA.

(c) **UK data transfers**. To the extent that Clarivate is based outside the UK and receives Client Personal Data protected under the UK GDPR, but no adequacy finding under the UK adequacy regulations applies, the parties agree to enter into the EU SCCs in the form as set out under Section 6(b) amended by the UK Addendum which shall be deemed incorporated to this DPA by reference.

(d) **FADP data transfers.** To the extent that Clarivate is based outside Switzerland and receives Client Personal Data protected under the FADP, but no adequacy decision under the FADP applies, the parties agree to enter into the EU SCCs in the form as set out under Section 6(b) which shall be amended as follows: (i) the references to the GDPR are to be construed as references to the corresponding provisions in the FADP, (ii) the references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be, (iii) the competent supervisory authority to be named in Annex B is the Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, (iv) Swiss law shall apply (Clause 17), (v) the choice of forum and jurisdiction in Clause 18 shall be Switzerland, and (vi) the term "Member State" in Clause 18(c) shall not be construed in a way to exclude data subjects having their place of residence in Switzerland from claiming for compensation.

(e) **Alternative Transfer Mechanism**. In the event that Clarivate implements or adopts alternative data transfer mechanisms as set forth under the Data Protection Laws (including any new version of or successor to the EU SCCs) for the transfer of Client Personal Data in compliance with the Data Protection Laws (hereinafter collectively referred to as "**Alternative Transfer Mechanisms**"), such Alternative Transfer Mechanism shall apply instead of the applicable transfer mechanisms described in this DPA. If and to the extent that a court of competent jurisdiction or supervisory authority orders (for whatever reason) came to the result that the measures described in this DPA cannot be relied on to lawfully transfer Client Personal Data in accordance with Data Protection Laws, Clarivate may implement any additional measures or safeguards that may be reasonably required to enable the lawful transfer of Client Personal Data.

7. Return or Deletion of Data

Upon termination or expiration of a Service and upon Client's written request and election made within thirty (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. This requirement shall not apply (i) to the extent Clarivate is required by applicable laws and regulations 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; or (iii) to Client Personal Data that Clarivate processes as a separate independent controller, as set out in Section 2.

8. Assistance with Data Subject Rights and Other Obligations under Data Protection Laws

(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 and to fulfil its obligations under Data Protection Laws to respond to requests from data subjects exercising their data subject's rights under Data Protection Laws at no additional cost. If required, taking into account the nature of the processing, Clarivate shall provide further reasonable assistance to Client to fulfil its obligations under Data Protection Laws to respond to requests from data subjects exercising their data subject's rights under Data Protection Laws. If any such request is made to Clarivate directly, Clarivate shall seek to obtain the Client's prior authorization to 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 confirm which of Clarivate's clients it is related to) or if required by applicable law. If Clarivate responds to such a request, Clarivate shall notify Client and provide Client with a copy of the request unless Clarivate is legally prohibited from doing so or deems this to be impractical, unreasonable as being of no or low interest to Client or a breach of applicable law.

(b) **Obligations under Data Protection Laws**. To the extent required under Data Protection Laws, and always exclusively in connection with the Services, Clarivate shall (taking into account the nature of the processing and the information available to Clarivate) provide a reasonable level of assistance to enable Client to ensure compliance with its obligations under Data Protection Laws, e.g., to carry out data protection impact assessments.

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 C, then the terms specified in Appendix C 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. However, for the purposes of clarity, this provision shall not limit any rights of data subjects under the EU SCCs (as modified for purposes of the UK GDPR and the FDPA).

(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.

Appendix A – Details of Data Processing

This Appendix A outlines the specific details of data processing activities where Clarivate acts as a processor and Client as a controller.

Data controller:

Client as defined in the Agreement.

Processor:

Clarivate as defined in the introducing sentence 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 processing as necessary: (i) to provide the Services in accordance with the Agreement; (ii) to fulfil Clarivate's contractual obligations under the Agreement and this DPA; (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; (iv) to keep the Services up to date and performant, to enhance user productivity, reliability, efficiency, quality and security; (v) to fix bugs and troubleshoot issues with the services; and (vi) 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	• Employees, agents, advisors and contractors of controller • Individuals authorized by controller to use the Services • Members of the academic community such as peer reviewers, editors of participating journals • Other data subjects as determined by controller	• Name and other non-sensitive identifiers such as employee ID number, ResearcherID, username) • Demographic information • Business contact information • Professional information • Other categories of personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement

Discovery, Research and Library Workflow Solutions:
360 Core
360 LINK
360 MARC Updates
360 Resource Manager
360 Search
Intota™ Assessment
Pivot/Pivot-RP
RefWorks
Summon
Ulrichsweb
Ulrich's™ Serials Analysis System
Intota™
	Hosting, implementation and/or technical support	• library patrons, library staff, faculty, students, administrators, employee s, visitors and alumni	• Basic user and patron information, including
			  • First and last names
			  • Postal addresses
			  • Email addresses
			  • Telephone numbers and other contact information
			  • Institutional identification numbers
			  • Department and Role
			• Basic staff and staff contact information
			• Staff related usage information, including records of staff operations and activity
			• Research activity
			• General usage information, including connection data (e.g., IP addresses)
			  • Suppliers/vendors information

EndNote	Hosting, technical support and associated services	• Employees, agents, advisors and contractors of controller (who are natural persons) • Members of the academic community such as publication authors and peer reviewers • Customers • Potential Customers • Other data subjects as determined by the controller	• Name and other non-sensitive identifiers such as email address, ResearcherID, and username Other categories of personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement
First to File	User account pre-registration; hosting; implementation and/or technical support; and professional services as applicable	• Employees, agents, advisors, freelancers of controller (who are natural persons) • Individuals authorized by controller to use the Services • Prospects, customers, business partners and vendors of controller (who are natural persons) • Employees or contact persons of controller's prospects, customers, business partners and vendors • Other data subjects as determined by controller including inventors, patent applicants and assignees, trademark owners, attorneys	• Name and other non-sensitive identifiers such as signatures • Business Contact information • Demographic information • Professional information • Other categories of personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement
Integrated Library Systems: **Millennium** **Polaris** **Sierra** **Vega** **Virtua** **and associated modules**	Hosting (unless hosted by the controller or an authorized third-party hosting provider), implementation and/or technical support	• Employees, agents, advisors, freelancers of controller (who are natural persons) • Individuals authorized by controller to use the Services, including library patrons	• 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 • 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) • Interactions with library staff • Use of other library services; information provided to

			facilitate any payments; and any late fees or fines • Name and other non-sensitive identifiers such as employee ID number and username • Business Contact information • Demographic information • Professional information • Other categories of personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement
IP management systems: **FoundationIP** **Ipfolio** **Ipendo** **Inprotech** **Memotech** **Patrawin** **The IP Management System** **Unycom**	Hosting (unless hosted by the controller or an authorized third-party hosting provider such as Salesforce), implementation and/or technical support	• Employees, agents, advisors, freelancers of controller (who are natural persons) • Individuals authorized by controller to use the Services • Prospects, customers, business partners and vendors of controller (who are natural persons) • Employees or contact persons of controller's prospects, customers, business partners and vendors • Other data subjects as determined by controller including inventors, patent applicants and assignees, trademark owners, attorneys	• Name and other non-sensitive identifiers such as employee ID number and username • Business Contact information • Demographic information • Professional information • Other categories of personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement
IP Professional Services	Provision of IP-related professional services including without limitation renewals, docketing and filing services	• Employees, agents, advisors, freelancers of controller (who are natural persons) • Individuals authorized by controller to use the Services • Prospects, customers, business partners and vendors of controller (who are natural persons) • Employees or contact persons of controller's prospects, customers, business partners and vendors • Other data subjects as determined by controller including inventors, patent applicants and assignees, trademark owners, attorneys	• Name and other non-sensitive identifiers such as employee ID number and username • Business Contact information • Demographic information • Professional information • Other categories of personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement
Market research – Contractually required safety and quality reporting as part of a market research engagement	Reporting to Client or Market Authorization Holder of safety and quality events as set forth in the Agreement	• Market research participants	• Name • Demographic information • Professional information • Contact information • Information required to process honoraria
Market research – List-based recruiting for primary market research projects	Handling of list provided by Client for the purposes of recruiting specific individuals for primary market research	• Potential market research participants	• Name • Demographic information • Contact information • Professional information • Information required to process honoraria

My Organization (InCites Benchmarking and Analytics Module)	Enabling Client to upload, analyze and manage its researchers' database on the Clarivate's My Organization modules of InCites	• Employees, agents, advisors and contractors of controller (who are natural persons) • Individuals authorized by controller to use the Services • Other data subjects as determined by controller	• Name and other non-sensitive identifiers such as employee ID number, ResearcherID, username • Demographic information • Business contact information • Professional information • Other categories personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement

Cloud-based library management, discovery, research, reading list and mobile/web app (Ex Libris SaaS services):
Alma
Esploro
CampusM
Leganto
Primo SaaS/Primo VE
Rapido
	Hosting, implementation, technical support and/or other related services	• Library patrons, library staff, faculty, students, administrators, employees, researchers, visitors and alumni	• Basic user and patron information, including
			  • First and last names
			  • Postal addresses
			  • Email addresses
			  • Telephone numbers and other contact information
			  • Institutional identification numbers
			• Library/catalogue related user and patron information, including
			  • Library activity, loans and fines information
			• Basic staff information, including contact information
			• Staff related usage information, including records of staff operations and activity
			• Research activity
			• General usage information, including connection data (e.g., IP addresses)
			• Suppliers/vendors information
			• Mobile Platform information, if applicable
			  • Device information (e.g., identifier and platform)
			• Attendance and location data, if applicable

Software Support and Maintenance Services for Locally Installed Ex Libris Software, including: **Aleph Local** **Primo Local** **Rosetta Local** **Voyager Local** **SFX**	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	• 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 • 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
Web of Science Reviewer Recognition; **Web of Science Author Connect** **Web of Science Reviewer Locator**	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	• Name and other non-sensitive identifiers such as ResearcherID • Demographic information • Business contact information • Professional information • Other information associated with the data • subjects' peer review activities
ScholarOne	Hosting, technical support and associated services	• Employees, agents, advisors and contractors of controller (who are natural persons) • Members of the academic community such as publication	• Name and other non-sensitive identifiers such as employee ID number, ResearcherID, username • Demographic information • Business contact information • Professional information

	authors and peer reviewers • Other data subjects as determined by controller	• Other categories personal data added to, generated by, or otherwise stored in the Services as permitted under the Agreement

Special Categories of Personal 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 makin g 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© 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 24×7 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 – Jurisdiction-Specific Terms

European Economic Area, UK, and Switzerland:

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 European Economic Area, the UK, or Switzerland, 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 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.

United States, California:

This "United States, California" section of Appendix C shall only apply and bind the parties if, and only to the extent that, Clarivate processes Client Personal Data under the scope of the CCPA. This "United States, California" section of Appendix C prevails over any conflicting terms of the Agreement or DPA, but does not otherwise modify the Agreement or DPA. The parties agree as follows:

(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 Appendix C only, "**Permitted Purposes**" shall include processing Client Personal Data only for the limited and specified business 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, and as otherwise agreed in writing, including, without limitation, in the Agreement, or as otherwise may be permitted for Service Providers under the CCPA.

(b) **Compliance.** Clarivate will comply with applicable sections of the CCPA, including providing the same level of privacy protection as required of Businesses by the CCPA. Clarivate may notify the Client after it makes a determination that it can no longer meet its obligations under the CCPA. Client may take reasonable and appropriate steps to ensure that Clarivate uses the Client Personal Data in a manner consistent with the Client's obligations under the CCPA. Client may, upon advance written notice, take reasonable and appropriate steps to stop and remediate any Clarivate's unauthorized use of Client Personal Data.

(c) **Prohibited Uses.** Clarivate will not

- "sell" or "share," as those terms are defined by the CCPA, Client Personal Data collected pursuant to the Agreement;
- retain, use, or disclose Client Personal Data for a business or commercial purpose other than as specified in the Agreement and this DPA;
- retain, use, or disclose Client Personal Data outside the direct business relationship with Client unless expressly permitted by applicable Data Protection Laws or regulations; or
- combine the Client Personal Data with Personal Information received from, or on behalf of, another person or persons, or collected from Clarivate's own interaction with a Consumer, except as permitted under the CCPA.

United States, Student Data – Family Educational and Privacy Rights (FERPA):

This "United States, Student Data" section of Appendix C shall only apply and bind the parties if, and only to the extent that, Clarivate processes Client Personal Data under the scope of FERPA ("**FERPA Data**") where the Client is an educational agency or institution to which regulations under FERPA apply. This "United States, Student Data" section of Appendix C prevails over any conflicting terms of the Agreement or DPA, but does not otherwise modify the Agreement or DPA. The parties agree as follows:

(a) Client will be responsible for providing any notifications and obtaining any parental consents that may be required by

applicable law with respect to Clarivate's processing of FERPA Data.

(b) Consistent with 34 CFR § 99.31(a)(1)(i), Clarivate shall not disclose FERPA Data to any other party, except as authorized by the Agreement or this DPA, as otherwise authorized in writing by the Client, or as required by applicable law. For the avoidance of doubt, Client agrees that Clarivate may disclose FERPA Data to its Sub-processors for the purposes of providing the Services.

Last Update: June 2025 (Version 3.0)