Clarivate™

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 that incorporates this DPA and under which Clarivate provides one or more of the Services to Client.

(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 (Cth) of Australia, as amended ("Australian Privacy Law"); and the UK Data Protection Act 2018, together with any implementing regulations ("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 SCCs.

(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 SCCs**" means the standard contractual clauses for processors as approved by the UK Information Commissioner's Office.

The terms "**personal data**", "**controller**", "**data subject**", "**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 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.

(b) Purpose limitation. Clarivate shall process Client Personal Data only in accordance with Client's documented lawful instructions as set forth in this DPA, as necessary to comply with applicable law, or as otherwise agreed in writing ("Permitted Purposes"). The parties agree that 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.

(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 promptly 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. If Client objects to the engagement of a new Sub-processor on reasonable grounds within ten (10) days, 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. If Clarivate is unable to provide an alternative, Client may terminate only the affected Services and receive a refund of prepaid fees 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, 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. 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) Audit rights. Upon at least 30 days written notice by Client, Clarivate shall make available to Client all information reasonably necessary to demonstrate compliance with this DPA and as required by Data Protection Laws, allow for and contribute to audits, including inspections by Client in order 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 the Clarivate or its third-party Sub-processors for any such audit. 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.

(b) Client audits. To the extent Clarivate or a Sub-processor holds a System and Organization Controls (SOC) 2 report, System and Organization Controls (SOC) 3 report or ISO 27001 certification that covers the Services, Client agrees to exercise any right Client may have to conduct an audit or inspection under Section 5(a) of 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.

6. International Transfers

(a) Data center locations. Subject to Sections 6(b) and 6(c), 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. Clarivate shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws and this DPA.

(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 that Clarivate is a recipient of Client Personal Data protected by UK Data Protection Law ("UK Data") in a country outside of the UK that is not recognized as providing an adequate level of protection for personal data (as described in applicable UK Data Protection Law), the parties agree to abide and by and process UK Data in compliance with the UK SCCs in the form set out in Appendix D. For the purposes of the descriptions in the UK 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 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 the Agreement and upon Client's written request and election, Clarivate shall (at Client's election) delete or return to Client all Client Personal Data (including copies) in its possession or control. This requirement shall not apply (i) to the extent Clarivate is required by applicable law to retain some or all of the Client Personal Data; or (ii) to Client Personal Data Clarivate has archived on back-up systems, which Client Personal Data 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 additional 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, 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.

Appendix A – Details of Data Processing

Controller (data exporter):
The Client and/or any Authorized Affiliates who qualify as controller under the terms of this DPA.

Processor (data importer):
The Clarivate entity and/or any Clarivate 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 (Return or Deletion of Data) 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 fulfill Clarivate's obligations under the Agreement and this DPA; and (iii) to comply with any other reasonable instructions provided by controller (e.g., via email or support tickets) that are consistent with the terms of the Agreement and (iv) as set forth by 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, the extent of which is determined and controlled by controller in its sole discretion, and which may include, but is not limited to the categories of Personal Data set forth by Service below.

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
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	• 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

		applicants and assignees, trademark owners, attorneys	
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

Publons Reviewer Connect	Only for handling lists (provided by Client) of individuals who will be invited to sign up to Publons	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 authors and peer reviewers • 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

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

Period of Retention:

Data will be retained for the duration of the Agreement and as outlined in Section 7 of the DPA.

The descriptions above also apply to Clarivate's transfers to subprocessors.

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 aligned to well-known industry standard ISO 27001 to protect the confidentiality, integrity and availability of its 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 on best practices relating to data security.

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.

User Access management

Clarivate has a well-defined process for granting access to all information assets. Privileges and access rights are granted to employees based on "Need-to-know" and "Least-privilege" principles to protect information assets against unauthorized access and disclosure. Clarivate password policy is enforced across the board on all information assets, which ensures 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 strong encryption. Clarivate has secured its perimeter with state of art Network Intrusion Prevention Systems (NIPS), Application Firewalls and Network based Firewalls.

There are tiered controls, including the use of network segmentation, to ensure the appropriate level of protection to systems and data. Data Loss Prevention controls are also deployed for email security.

Endpoint and virus protection

In line with our policies, all Clarivate owned and supported operating systems which are hosted in our data centers or deployed in the cloud are required to be configured with our 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. At times, additional security controls may be implemented to provide mitigation against known threats.

Security monitoring

Automated and systemic centralized security logging and monitoring of the operating environment is ongoing through our SOC (Security Operation Center) for the purpose of real-time awareness, event correlation and incident response.

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. The plan is implemented according to various recognized standards and industry best practices such as: 1) NIST Computer Security Incident Handling Guide, 2) VERIS Community Database (VCDB) and 3) Verizon Data Breach Investigations Report (DBIR).

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.

Device lockdown

Standard security builds are deployed across our infrastructure with our security agents installed. Our server builds are based on industry practices for secure configuration Management.

Operations Security

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

Clarivate ensures backup copies of information and software are 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 ensure the health of our operating environments. Management tools are implemented to monitor and maintain an appropriately scaled and highly available environment.

Vulnerability scanning

Our Information Security Team supports a vulnerability scanning and policy compliance service that product and technology teams utilize for internal and external vulnerability scanning and configuration compliance. Internet-facing sites on our global network are periodically scanned as a practice in our program focused on vulnerability management.

Risk assessment

Our product and technology teams engage information security subject matter experts regularly to provide risk assessments services. Architecture reviews, external 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 data centers including cloud service providers where the majority of application products are deployed and managed to the standards, and industry best practice 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 data centers 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 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 D*a*ta 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 subprocessing 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 Standard Contractual Clauses (Processor)

In accordance with applicable data protection law, including the Retained Regulation (EU) 2016/679 ("UK GDPR"), Clarivate (hereinafter the "data importer") and Client (hereinafter the "data exporter") each a “party”; together “the parties”, HAVE AGREED on the following Contractual Clauses (the Clauses) 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 data exporter to the data importer of the personal data specified in Annex 1.

Clause 1

Definitions

For the purposes of the Clauses:

a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'Commissioner'* shall have the same meaning as in the UK GDPR;
b) *'the data exporter'* means the controller who transfers the personal data;
c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;
d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;
f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Annex 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations

of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law;
b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Annex 2 to this contract;
d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
e) that it will ensure compliance with the security measures;
f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;
g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension;
h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Annex 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[1]

The data importer agrees and warrants:

a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly 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 contract;

b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c) that it has implemented the technical and organisational security measures specified in Annex 2 before processing the personal data transferred;

d) that it will promptly notify the data exporter about:

   i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

   ii. any accidental or unauthorised access, and

   iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;

f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;

g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
    a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;
    b) to refer the dispute to the UK courts.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the country of the UK in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

ANNEX 1 TO THE UK STANDARD CONTRACTUAL CLAUSES

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.

Data subjects:

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

Categories of data:

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

Processing operations:

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

ANNEX 2 TO THE UK STANDARD CONTRACTUAL CLAUSES

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

As set forth in Appendix B of the DPA to which these Clauses are appended.

ANNEX 3 TO THE UK STANDARD CONTRACTUAL CLAUSES

The parties acknowledge that Clause 10 of the Clauses permits them to include additional business-related terms provided they do not contradict with the Clauses. 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 4(h) and 8: 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 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a) and Clause 5(b): Suspension of data transfers and termination

1. The parties acknowledge that for the purposes of Clause 5(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 5(a) and/or Clause 5(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 5(f): Audit

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

Clause 5(j): 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 subprocessing agreement to data exporter.

Clause 6: 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 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.