CORELIGHT DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedules and the Standard Contractual Clauses ("**DPA**") forms part of the Corelight Customer Agreement or other written agreement entered between Customer and Corelight governing Customer's use of the Corelight Offerings (as defined below) entered into between Customer and Corelight ("**Agreement**") and applies solely to the extent Corelight processes any Personal Data (as defined below) in connection with the Corelight Offerings. Capitalized terms used and not defined in this DPA have the meanings given to them in the Agreement, of if not defined in the Agreement, in the Corelight Customer Agreement located at www.corelight.com/legal/agreements (or such successor URL as may be designated by Corelight).

1. **DEFINITIONS**.

"**Applicable Data Protection Law**" means all data protection and privacy laws and regulations applicable to the processing of Personal Data under the Agreement, as they may be amended or otherwise updated from time to time, including, where applicable, the European Data Protection Laws and US Data Protection Laws.

"**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended, including its implementing regulations and the California Privacy Rights Act of 2020.

"**Corelight Offerings**" means the Cloud Products and/or any other Services (e.g., Consulting Services or Support Services) provided directly by Corelight to Customer under the Agreement.

"**Covered Data**" means Personal Data that is (a) provided by or on behalf of Customer to Corelight in connection with the Corelight Offerings; or (b) obtained, developed, produced or otherwise processed by Corelight, or its agents or subcontractors, for purposes of providing the Corelight Offerings, in each case as further described in Schedule 1.

"**Customer**" means the entity identified as the "Customer" in the Agreement and this DPA.

"**Data Subject**" means a natural person whose Personal Data is processed.

"**Deidentified Data**" means data created using Covered Data that cannot reasonably be linked to such Covered Data, directly or indirectly.

"**European Data Protection Laws**" means (a) Regulation 2016/679 (General Data Protection Regulation) ("**EU GDPR**"); (b) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); and (c) the Swiss Federal Data Protection Act and its implementing regulations ("**Swiss Data Protection Act**"); in each case as may be amended, superseded or replaced from time to time.

"**Personal Data**" means any 'personal data', 'personal information' or 'personally identifiable information' contained within Customer Data or provided to Corelight for processing under the Agreement by or on behalf of Customer in the provision of the Corelight Offerings.

"**Restricted Transfer**" means a transfer (directly or via onward transfer) of personal data that is subject to European Data Protection Laws to a third country outside the European Economic Area, United Kingdom and Switzerland which is not subject to an adequacy determination by the European Commission, United Kingdom or Swiss authorities (as applicable).

"**Security Breach**" means any breach of Corelight's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data on systems managed by or otherwise controlled by Corelight. Security Breaches will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Security Measures**" means the then-current applicable technical and organizational security measures for a Corelight Offering, available at www.corelight.com/trust-center (or a successor website designated by Corelight).

"**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, as may be amended, superseded or replaced from time to time.

"**Subprocessor**" means any other processor engaged by Corelight (including any Corelight affiliate) to process Personal Data.

The terms "**controller**", "**data subject**", "**supervisory authority**", "**processor**", "**process**", "**processing**", "**personal data**", and "**personal information**" will have the meanings given to them in Applicable Data Protection Laws. The term "controller" includes "business", the term "data subject" includes "consumers", and the term "processor" includes "service provider" (in each case, as defined by the CCPA).

2. PROCESSING OF PERSONAL DATA.

2.1. **Roles of the Parties**. This DPA applies when Personal Data is processed by Corelight as either a processor or subprocessor in its provision of the Corelight Offerings to Customer, who will act as either a controller or processor of Personal Data.

2.2. **Details of Processing**. The details of the processing of Personal Data by Corelight are set out in Schedule 1 to this DPA.

2.3. **Corelight's Processing**. Corelight will process Personal Data only in accordance with Customer's documented lawful instructions. For these purposes, Customer instructs Corelight to process Personal Data for the following purposes: (a) processing in accordance with the Agreement; (b) processing initiated by Customer in its use or configuration of the Corelight Offerings; and (c) processing to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement. Customer will ensure that its instructions comply with Applicable Data Protection Law. Corelight will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate Applicable Data Protection Law. Without limiting the foregoing, Corelight is prohibited from (1) selling Covered Data or otherwise making Covered Data available to any third party for monetary or other valuable consideration; (2) sharing Covered Data with any third party for cross-context behavioral advertising; (3) retaining, using, or disclosing Covered data for any purpose other than the business purposes specified in the Agreement or otherwise permitted by Applicable Data Protection Laws; (4) retaining, using or disclosing Covered Data outside of the direct business relationship between the parties; and (5) except as otherwise permitted by Applicable Data Protection Laws, combining Covered Data with Personal Data that Corelight receives from or on behalf of another person or persons, or collects from its own interaction with the Data Subject.

2.4. **Compliance**. Customer represents and warrants that: (a) it has provided all applicable notices to data subjects and, to the extent required, obtained consent from data subjects in each case as required for the lawful processing of Personal Data in accordance with the Agreement and this DPA; and (b) it has complied and will continue to comply with Applicable Data Protection Law.

3. SECURITY.

3.1. **Confidentiality**. Corelight will ensure that: (a) Corelight's access to Personal Data is limited to those personnel who require such access to deliver the Corelight Offerings in accordance with the Agreement; and (b) all Corelight personnel authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.2. **Security Measures**. Corelight has implemented and will maintain the technical and organizational security measures as set out in the Security Measures. Customer is responsible for reviewing the Security Measures that Corelight makes available and independently determining that the Security Measures are appropriate to ensure the security of Personal Data and otherwise consistent with Customer's obligations under Applicable Data Protection Law. The Security Measures are subject to technical progress and development and Corelight may update the Security Measures, provided that any updates will not materially diminish the overall security of Personal Data or the Corelight Offerings. Corelight may make available certain security controls within the Corelight Offerings that Customer may use in accordance with the Documentation.

3.3. **Security Breach**. In the event of a Security Breach, Corelight will: (a) notify Customer in writing without undue delay after becoming aware of the Security Breach; and (b) promptly take reasonable steps to contain, investigate, and mitigate any adverse effects resulting from the Security Breach. Corelight will reasonably cooperate with and provide to Customer information in its possession to assist Customer in meeting Customer's obligations to report a Security Breach as required under Applicable Data Protection Law, taking into account the nature of the processing, the information available to Corelight, and any restrictions on disclosing the information (such as confidentiality). Corelight's notification of or response to a Security Breach under this Section will not be construed as an acknowledgement by Corelight of any fault or liability with respect to a Security Breach.

4. SUBPROCESSORS.

4.1. **Authorization**. Customer grants Corelight a general authorization for the use by each Corelight affiliate, as well as other third parties listed at www.corelight.com/legal/subprocessors (each a "**Subprocessor**") to receive and process Personal Data in accordance with this Section.

4.2. **Subprocessor Obligations**. When engaging any Subprocessor, Corelight will: (a) ensure that any Subprocessor accesses Personal Data only as necessary to perform the Corelight Offerings in accordance with the Agreement

and this DPA; (b) impose contractual data protection obligations to protect Personal Data in accordance with the standard required by Applicable Data Protection Law; and (c) remain liable for any breach of this DPA that is caused by any act, error or omission of its Subprocessors.

4.3. **Subprocessor Changes**. At least ten calendar days' prior to the date on which any new Subprocessor will commence processing Personal Data, Corelight will update the Subprocessor List and provide Customer with notice of that update. Such notice will be sent to: (a) Customer's contact details listed in Schedule 1; and (b) any individuals who have signed up to receive updates to the Subprocessor List via the mechanism(s) indicated on the Subprocessor List.

4.4. **Subprocessor Objections**. Customer may object to Corelight's use of a new Subprocessor (including when exercising its right to object under clause 9(a) of the SCCs if applicable) by providing Corelight with written notice of the objection within ten days after Corelight has provided notice to Customer of such proposed change (an "**Objection**"). Where Customer fails to object to such change within such period of time, Customer shall be deemed to have consented to such change. Where a materially important reason for such Objection exists and is provided in writing by Customer to Corelight at privacy@corelight.com within ten calendar days after receiving notice pursuant to Section 4.3, then Corelight will either: (a) work with Customer to address Customer's objections to its reasonable satisfaction; (b) instruct the Subprocessor to not process Personal Data; or (c) notify Customer of its option to terminate the Agreement with respect to only those Corelight Offerings which cannot be provided by Corelight without the use of the objected-to Subprocessor within a reasonable timeframe. During any such Objection period, Corelight may suspend the affected portion of the Corelight Offerings.

5. **PERSONAL DATA TRANSFERS**. Corelight may transfer Personal Data to any country or territory, as reasonably necessary for the provision of the Corelight Offerings, consistent with this DPA.

5.1. **Restricted Transfers**. Where the transfer of Personal Data to Corelight constitutes a Restricted Transfer, such transfer will be governed by the Standard Contractual Clauses, which will be deemed incorporated into and form an integral part of the Agreement in accordance with Schedule 2 of this DPA.

5.2. **Alternative Transfer Mechanism**. If and to the extent that a court of competent jurisdiction or a supervisory authority with binding authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer Personal Data to Corelight, the parties will reasonably cooperate to agree and take any actions that may be reasonably required to implement any additional measures or alternative transfer mechanism to enable the lawful transfer of such Personal Data. Additionally, in the event Corelight adopts an alternative transfer mechanism, such alternative transfer mechanism will apply instead of the SCCs described in Section 5.1of this DPA (but only to the extent such alternative transfer mechanism complies with applicable European Data Protection Laws and extends to the territories to which Personal Data is transferred).

6. **CERTIFICATIONS & AUDITS**.

6.1. **Certifications**. Where available and upon Customer's request, Corelight will provide Customer or Customer's authorized representatives certifications, attestations, reports or extracts thereof from third parties or other suitable certifications to demonstrate Corelight's compliance with Applicable Data Protection Law and the terms of this DPA (each, a "**Certification**"). Any Certification will be considered Corelight's Confidential Information and subject to appropriate confidentiality obligations.

6.2. **Audits**. Customer and/or Customer's authorized representatives may audit the Corelight delivery centers and Security Measures relevant to the Personal Data processed by Corelight only if: (a) Corelight notifies Customer of a Security Breach; (b) an audit is required by Customer's supervisory authority; or (c) where required by Applicable Data Protection Law or the SCCs and provided that Customer may only audit once in any twelve-month period unless Applicable Data Protection Law requires more frequent audits. Customer will provide at least sixty days advance notice of any audit unless Applicable Data Protection Law or a competent data protection authority requires shorter notice. Prior to beginning any audit, Corelight and Customer will mutually agree upon the reasonable start date, scope and duration of and security and confidentiality controls applicable to the audit in addition to allocation of costs between the parties. Corelight may object in writing to an auditor appointed by Customer to conduct any audit if the auditor is, in Corelight's reasonable opinion, not suitably qualified or independent or a competitor of Corelight. The scope of any audit will not require Corelight to disclose to Customer or Customer's authorized representatives, or to allow Customer or Customer's authorized representatives to access: (i) any data or information of any other Corelight customer; (ii) any Corelight internal accounting or financial information; (iii) any Corelight trade secret; or (iv) any information that, in Corelight's reasonable opinion could: (x) compromise the security of Corelight's systems or premises; or (y) cause Corelight

to breach its obligations under Applicable Data Protection Law or Corelight's security, confidentiality and/or privacy obligations to any other Corelight customer or any third party. Customer will promptly notify Corelight of any non-compliance discovered during an audit.

7. **COOPERATION & ASSISTANCE**.
   7.1. **Data Subject Requests**. Customer is responsible for responding to and complying with data subject requests ("**DSR**"). At Customer's request, Corelight will, taking into account the nature of the processing, reasonably cooperate with Customer to enable Customer to respond to the DSR. If a data subject sends a DSR to Corelight directly and where Customer is identified or identifiable from the request, Corelight will promptly forward such DSR to Customer and Corelight will not, unless legally compelled to do so, respond directly to the data subject except to refer them to the Customer to allow Customer to respond as appropriate.
   7.2. **Data Protection Impact Assessments**. At Customer's request, Corelight will provide reasonable cooperation to Customer in connection with any data protection impact assessment or consultations with regulatory authorities that may be required in accordance with Applicable Data Protection Law.
   7.3. **Legal Requests**. If Corelight receives a subpoena, court order, warrant or other legal demand from law enforcement or any public or judicial authority seeking the disclosure of Personal Data, Corelight will attempt to redirect the governmental body to request such Personal Data directly from Customer. As part of this effort, Corelight may provide Customer's basic contact information to the governmental body. If compelled to disclose Personal Data to a governmental body, then Corelight will give Customer reasonable notice of the legal demand to allow Customer to seek a protective order or other appropriate remedy, unless Corelight is legally prohibited from doing so.
8. **RETRIEVAL & DELETION OF PERSONAL DATA**. Corelight will enable Customer to retrieve and/or delete Personal Data during the term of the Agreement in a manner consistent with the functionality of the Corelight Offerings. Upon termination or expiration of the Agreement and following Customer's written request, Corelight will delete or assist Customer in deleting any Personal Data within Corelight's possession or control within thirty days following such request.
9. **CCPA COMPLIANCE**. Corelight will not process, retain, use, or disclose Personal Data for any purpose other than for the purposes set out in the Agreement, DPA and as permitted under the CCPA. Corelight will not sell or share information as those terms are defined under the CCPA.
10. **DEIDENTIFIED DATA**. If Corelight receives Deidentified Data from or on behalf of Customer, then Corelight will: (1) take reasonable measure to ensure the information cannot be associated with a Data Subject; (2) publicly commit to process the Deidentified Data solely in deidentified form and not attempt to reidentify the information; and (3) contractually obligate any recipients of Deidentified Data to comply with the foregoing requirements and Applicable Data Protection Laws.
11. **GENERAL**.
    11.1. The parties agree that this DPA will replace any existing data processing addendum, attachment, exhibit or standard contractual clauses that the parties may have previously entered into in connection with the Corelight Offerings. Corelight may update this DPA from time to time, with such updated version posted to www.corelight.com/legal/agreements (or a successor website designated by Corelight); provided, however, that no such update will materially diminish the privacy or security of Personal Data.
    11.2. If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.
    11.3. In the event of any conflict between this DPA and any data privacy provisions set out in any Agreement between the parties relating to the Corelight Offerings, the parties agree that the terms of this DPA will prevail, provided that if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses control and take precedence.
    11.4. This DPA will 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.
    11.5. The obligations placed upon each party under this DPA and the Standard Contractual Clauses will survive so long as Corelight processes Personal Data on behalf of Customer.

Schedule 1

DESCRIPTION OF PROCESSING TRANSFER

ANNEX 1(A): LIST OF PARTIES	
Data exporter	**Name of the data exporter**: The entity identified as the "Customer" in the Agreement and this DPA **Contact details**: The address and contact details associated with Customer's Corelight account, or as otherwise specified in this DPA or the Agreement **Activities relevant to the data transferred**: The activities specified in Annex 1.B below **Role (Controller/Processor)**: Controller (for Module 2) or Processor (for Module 3)
Data importer	**Name of the data importer**: Corelight, Inc. **Contact details**: privacy@corelight.com **Activities relevant to the data transferred**: The activities specified in Annex 1.B below **Role (Controller/Processor)**: Processor
ANNEX 1(B): DESCRIPTION OF THE PROCESSING / TRANSFER	
Categories of data subjects whose personal data is transferred:	Customer's end users (i.e., individuals permitted to access and use the Corelight Offerings on Customer's behalf), employees, customers, business partners, and suppliers (who are natural persons).
Categories of personal data transferred:	All data relating to individuals provided to Corelight via the Corelight Offerings, by (or at the direction of) Customer or by Customer's end users, including, but not limited to, the following: Cloud Products *Corelight Investigator* • Full name • Username • Email • Phone Number • Title • Location • IP address • Device name / hostname • Network activity • Wi-Fi • Serial number Support • Business contact details (name, email address and phone number) of the individual requesting Support • IP address • Troubleshooting files (meaning text, video or images files provided to Corelight by Customer in its discretion) Consulting Services As defined in the applicable statement of work
Special categories of personal data transferred (if relevant):	Not applicable

Frequency of the transfer:	Cloud Products Transfers will be made on a continuous basis Support Transfers will be made on a one-off basis when Customer submits a support case Consulting Services Transfers may be made on a continuous and/or one-off basis subject to the applicable statement of work
Nature, subject matter and duration of the processing:	**Nature:** Cloud Products Use and other processing activities (including collection, transmission, storage) of Personal Data to provide, maintain and update the Cloud Products Support Use and other processing activities (including collection, transmission, storage) of Personal Data to provide end user maintenance and support services to Customer Consulting Services Use and other processing activities (including collection, transmission, storage) of Personal Data to deliver Consulting Services as described in the applicable statement of work **Subject Matter:** Corelight will process Personal Data as necessary to provide the Corelight Offerings under the Agreement. **Duration:** The duration of the processing will be for the term of the Agreement and any period after the termination or expiry of the Agreement during which Corelight processes Personal Data.
Purpose(s) of the transfer and further processing:	Cloud Products Corelight's provision and support of the Cloud Products as described in the Agreement Support Corelight's provision of end user maintenance and support services as described in the Agreement Consulting Services Corelight's provision of training, consulting, implementation and other professional services as described in the applicable statement of work
Period for which the personal data will be retained:	Corelight will retain Personal Data for the term of the Agreement and any period after the termination of expiry of the Agreement during which Corelight processes Personal Data in accordance with the Agreement.
Subprocessors:	As described at www.corelight.com/legal/subprocessors
ANNEX 1(C): COMPETENT SUPERVISORY AUTHORITY	
Competent supervisory authority:	The data exporter's competent supervisory authority will be determined in accordance with the EU GDPR.

Schedule 2

STANDARD CONTRACTUAL CLAUSES (MODULES 2 AND 3)

1. Subject to Section 5.1 of the DPA, where the transfer of Personal Data to Corelight is a Restricted Transfer and Applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer will be governed by the SCCs, which will be deemed incorporated into and form part of the DPA as follows:

   1.1. In relation to the transfers of Personal Data protected by the EU GDPR, the SCCs will apply as follows:

   (a) Module Two terms will apply (where Customer is the controller of Personal Data) and the Module Three terms will apply (where Customer is the processor of Personal Data);

   (b) Clause 7 of the SCCs (Docking Clause) does not apply;

   (c) In clause 8.9, any audits will be carried out in accordance with Section 6.2 of the DPA;

   (d) In clause 9, option 2 ("**general authorization**") is selected, and the process and time period for prior notice of Subprocessor changes will be as set out in Section 4 of the DPA;

   (e) The option in Clause 11(a) of the SCCs (Independent dispute resolution body) does not apply;

   (f) In clause 17, option 1 will apply and the SCCs will be governed by law of the Republic of Ireland;

   (g) In clause 18(b), disputes will be resolved before the courts of the Republic of Ireland;

   (h) Annex I will be deemed completed with the information set out in Schedule 1 to the DPA; and

   (i) Annex II will be deemed completed with the information set out in the Security Measures, subject to Section 3.2 of the DPA.

   1.2. In relation to transfers of Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented under Section 1.1 above will apply with the following modifications:

   (a) references to "Regulation (EU) 2016/679" and specific articles therein will be interpreted as references to the Swiss Data Protection Act and the equivalent articles or sections therein;

   (b) references to "EU", "Union", "Member State" and "Member State law" will be replaced with references to "Switzerland" and/or "Swiss law" (as applicable);

   (c) references to the "competent supervisory authority" and "competent courts" will be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";

   (d) the SCCs will be governed by the laws of Switzerland; and

   (e) disputes will be resolved before the competent Swiss courts.

   1.3. In relation to transfers of Personal Data protected by the UK GDPR, the SCCs will apply pursuant to Schedule 3 (UK Supplement) of the DPA.

2. Where the SCCs apply pursuant to Section 5.1 of the DPA, this section sets out the parties' interpretations of their respective obligations under specific provisions of the SCCs, as identified below. Where a party complies with the interpretations set out below, that party will be deemed by the other party to have complied with its commitments under the SCCs:

   2.1. Where Customer is itself a processor of Personal Data acting on behalf of a third party controller and Corelight would otherwise be required to interact directly with such third party controller (including notifying or obtaining authorizations from such third party controller), Corelight may interact solely with Customer and Customer will be responsible for forwarding any necessary notifications to and obtaining any necessary authorizations from such third party controller;

   2.2. The certification of deletion described in clause 16(d) of the SCCs will be provided by Corelight to Customer upon Customer's written request; and

   2.3. For the purposes of clause 15(1)(a) the SCCs, Corelight will notify Customer and not the relevant data subject(s) in case of government access requests, and Customer will be solely responsible for notifying the relevant data subjects as necessary.

Schedule 3

UK SUPPLEMENT

1. This UK Supplement will apply in the event that: (a) Corelight processes Personal Data on the behalf of Customer as a processor in the course of providing the Corelight Offerings pursuant to the Agreement; and (b) Customer is subject to UK Data Protection Law and acts as a controller thereunder. In the event of a conflict or inconsistency between the Agreement or the DPA and this UK Supplement, this UK Supplement will prevail with respect to Personal Data from the United Kingdom, but solely with regard to the portion of the provision in conflict.
2. **DEFINITIONS**. All terms used herein but not defined in the DPA will have the meaning assigned to them in the applicable UK Data Protection Law. All references to Applicable Data Protection Law or laws in the DPA will be read in the context of UK Data Protection Law for the purpose of this UK Supplement.
   2.1. "**Mandatory Clauses**" means Part 2: Mandatory Clauses of the UK Addendum, as it is revised under Section 18 of those Mandatory Clauses.
   2.2. "**Standard Contractual Clauses**" means the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
   2.3. "**UK Addendum**" means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioners Office under S.119 (a) of the UK Data Protection Act 2018, as updated or amended from time to time.
   2.4. "**UK Data Protection Law**" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the United Kingdom, including: (a) the UK GDPR and UK Data Protection Act 2018; and/or (b) other laws that are similar, equivalent to, successors to, or that are intended to or implement the laws that are identified in (b) above.
3. **INTERNATIONAL TRANSFERS**.
   3.1. To the extent that Corelight processes any Personal Data from the United Kingdom and transfers such Personal Data outside of the United Kingdom to countries not deemed to provide an adequate level of data protection under UK Data Protection Law, the parties agree to enter into and comply with the Standard Contractual Clauses (as amended by the Mandatory Clauses), as discussed in Section 4 of this UK Supplement. Corelight agrees that it is a "data importer" and Customer is the "data exporter" under the Standard Contractual Clauses (as amended by the Mandatory Clauses).
   3.2. The parties agree that the data export solution identified in Section 4.1 (Mandatory Clauses) will not apply if and to the extent that Corelight adopts an alternative data export solution for the lawful transfer of Personal Data (as recognized under UK Data Protection Law) outside of the United Kingdom, in which event, Customer will take any action (which may include execution of documents) strictly required to give effect to such solution and the alternative transfer mechanism will apply instead (but only to the extent such alternative transfer mechanism extends to the territories to which Personal Data is transferred).
4. **MANDATORY CLAUSES**.
   4.1. The Mandatory Clauses are incorporated by reference into this UK Supplement and the Standard Contractual Clauses are amended in accordance with the Mandatory Clauses.
   4.2. Neither the Mandatory Clauses nor this UK Supplement will be interpreted in a way that conflicts with rights and obligations provided for under UK Data Protection Law.
   4.3. Corelight (as data importer) may end this DPA (including this UK Supplement) to the extent the Mandatory Clauses apply, in accordance with Section 19 of the Mandatory Clauses.
   4.4. For the purposes of this UK Supplement, the following will apply and will be read and interpreted in accordance with the Mandatory Clauses:
      (a) Module Two of the Standard Contractual Clauses will apply.
      (b) In respect to clause 9(a) *Sub-processors*, Customer grants Corelight General Written Authorization for the use of Subprocessors. A list of Corelight's Subprocessors is available at www.corelight.com/legal/subprocessors.
   4.5. In respect to clause 17 *Governing Law*: the governing law is that of England and Wales.
   4.6. In respect to clause 18 *Choice of forum and jurisdiction*: The courts of England and Wales will resolve any disputes arising from the Standard Contractual Clauses (as amended by the Mandatory Clauses).
   4.7. Tables 1, 2 and 3 in Part 1 of the UK Addendum will be deemed completed with the information set out in Schedule 1 to the DPA and the Security Measures respectively, and Table 4 in Part 1 of the UK Addendum will be deemed completed by selecting "neither party".