

DATA PROTECTION ADDENDUM

This Data Protection Addendum (“DPA”) is entered into as of the Effective Date (defined below) between Silverchair Science+Communications LLC (“Silverchair”) and the entity that has subscribed to the Services (“Customer”) pursuant to, and as set forth in, the Master Services Agreement (“MSA”, or the “Agreement”). Silverchair and Customer may each be referred to as a “Party” and or collectively referred to as the “Parties”. To the extent of any conflict or inconsistency between this DPA and the remaining terms of the Agreement, this DPA will govern. The “Effective Date” of this DPA shall be the Effective Date of the Agreement.

1. Definitions

“California Personal Information” means Personal Data that is subject to the protection of the CCPA.

“CCPA” means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).

“Consumer”, “Business”, “Sell” and “Service Provider” will have the meanings given to them in the CCPA.

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Data Protection Laws” means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws, the CCPA and the data protection and privacy laws of Australia and Singapore; in each case as amended, repealed, consolidated or replaced from time to time.

“Data Subject” means the individual to whom Personal Data relates.

“Europe” means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

“European Data” means Personal Data that is subject to the protection of European Data Protection Laws.

“European Data Protection Laws” means data protection laws applicable in 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; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms part of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (“UK GDPR”); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance (“Swiss DPA”); in each case, as may be amended, superseded or replaced.

“Personal Data” means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data, personal information or personally identifiable information under applicable Data Protection Laws.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by us and/or our Subprocessors in connection with the provision of the Services.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms “Process”, “Processes” and “Processed” will be construed accordingly.

“Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

“Standard Contractual Clauses” means the standard contractual clauses annexed to the European Commission’s Decision (EU) 2021/914 of 4 June 2021, in the form set out at Annex A; as may be amended, superseded or replaced.

“Subprocessor” means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the provision of the Services under the Agreement.

2. Scope and Relationship of the Parties

This DPA applies only to the *Personal Data that Silverchair receives in the Services from or on behalf of Customer or Customer's Authorized Users*.

For such Personal Data, Customer is (or represents that it is acting with full authority on behalf of) the "Controller", and Silverchair is the "Processor", as such terms are defined in the GDPR (regardless of whether the GDPR applies).

3. Silverchair's Responsibilities

Silverchair will retain, use, disclose, and otherwise Process the Personal Data only as described in the Agreement, unless obligated to do otherwise by Applicable Law. In such case, Silverchair will inform Customer of that legal requirement before the Processing unless legally prohibited from doing so. Without limiting the foregoing:

- Silverchair will not retain, use, disclose, or otherwise Process the Personal Data in a manner inconsistent with Silverchair's role as Customer's "Service Provider", as such term is defined in the CCPA (regardless of whether the CCPA applies);
- Silverchair will not "sell" the Personal Data, as such term is defined in the CCPA (regardless of whether the CCPA applies);
- Silverchair hereby certifies that it understands the restrictions and obligations set forth in this DPA and that it will comply with them.

The details of the Processing are set forth in Annex 1 to the Standard Contractual Clauses.

4. Customer's Instructions to Silverchair

Customer will not instruct Silverchair to Process Personal Data in violation of Applicable Law. Silverchair has no obligation to monitor the compliance of Customer's use of the Services with Applicable Law, though Silverchair will promptly inform Customer if, in Silverchair's opinion, an instruction from Customer with respect to Personal Data subject to the GDPR infringes the GDPR or other EU (or EU Member State) data protection provisions.

The Agreement, including this DPA, along with Customer's configuration of any settings or options in the Services (as Customer may be able to modify from time to time), constitute Customer's complete and final instructions to Silverchair regarding the Processing of Personal Data, including for purposes of the Standard Contractual Clauses.

5. Subprocessors

Silverchair may subcontract the collection or other Processing of Personal Data in compliance with Applicable Law to provide the Services. Prior to a Subprocessor's Processing of Personal Data, Silverchair will impose contractual obligations on the Subprocessor that are substantially the same as those imposed on Silverchair under this DPA. Subprocessor security obligations will be deemed substantially the same if they provide a commercially reasonable level of security even if the Subprocessor does not follow the security certifications that Silverchair does.

Subprocessors are listed at www.silverchair.com/legal/subprocessors (the "**Subprocessor List**"). When any new Subprocessor is engaged, Silverchair will make an updated Subprocessor List available at least 15 business days before the new Subprocessor Processes any Personal Data, unless exigent circumstances require earlier Processing of Personal Data, in which case they will be added as soon as practicable. This paragraph constitutes Customer's consent to the Subprocessor List, as well as any subprocessing under the Standard Contractual Clauses, if they apply. The Subprocessor agreements to be provided under the Standard Contractual Clauses may have all commercial information, or provisions unrelated to the Standard Contractual Clauses, redacted prior to sharing with Customer, and Customer agrees that such copies will be provided by Silverchair only upon request.

Customer's sole recourse if it objects to a Subprocessor will be to terminate the Agreement. Following such termination, Customer will be entitled to a refund of unused prepaid fees. This is without prejudice to any right Customer may have under the Agreement to termination for breach of contract.

Silverchair remains liable for its Subprocessors' performance to the same extent Silverchair is liable for its own performance, consistent with the limitations of liability set forth herein.

6. Security

Silverchair will assist Customer in Customer's compliance with the security obligations of the GDPR and other Applicable Law, as relevant to Silverchair's role in Processing the Personal Data, taking into account the nature of Processing and the information available to Silverchair, by implementing technical and organizational measures that comply with Annex B, without prejudice to Silverchair's right to

make future replacements or updates to the measures that do not lower the level of protection of Personal Data.

Silverchair will ensure that the persons Silverchair authorizes to Process the Personal Data are subject to a written confidentiality agreement covering such data or are under an appropriate statutory obligation of confidentiality.

7. Personal Data Breach Notification

Silverchair will comply with the Personal Data Breach-related obligations directly applicable to it under the GDPR and other Applicable Law. Taking into account the nature of Processing and the information available to Silverchair, Silverchair will assist Customer in complying with those applicable to Customer by informing Customer of a confirmed Personal Data Breach without undue delay, and in no case more than 48 hours after becoming aware. Any such notification is not an acknowledgement of fault or responsibility. To the extent available, this notification will include Silverchair's then-current assessment of the following, which may be based on incomplete information:

- The nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of Personal Data records concerned;
- The likely consequences of the Personal Data Breach; and
- Measures taken or proposed to be taken by Silverchair to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects.

Nothing shall be construed to require Silverchair to violate, or delay compliance with, any legal obligation it may have with respect to a Personal Data Breach or other security incidents generally.

8. Data Subject Requests

Taking into account the nature of the Processing, Silverchair will provide reasonable assistance to Customer for the fulfilment of Customer's obligation to honor requests by individuals to exercise their rights under the GDPR and other Applicable Law (such as rights to access their Personal Data) and will notify Customer of any such requests or Personal Data-related complaints from an individual that Silverchair receives. Silverchair will send this within a commercially reasonable timeframe, which shall will not exceed 5 business days if (i) the request or complaint is received through the contact information specified in the Silverchair privacy policy that is linked from the home page of <https://www.silverchair.com> and (ii) the request or complaint identifies Customer as the Silverchair customer to whom it pertains. Although it is Customer's responsibility to respond to and honor data subjects' requests in compliance with law, Silverchair does not waive any rights under the Agreement to remove content from the Services.

9. Assistance with DPIAs and Consultation with Supervisory Authorities

Taking into account the nature of the Processing and the information available to Silverchair, Silverchair will provide reasonable assistance to and cooperation with Customer for Customer's performance of any legally required data protection impact assessment of the Processing or proposed Processing of the Personal Data involving Silverchair, and with related consultation with supervisory authorities, by providing Customer with any publicly available documentation for the relevant Services or by complying with the Audit section below. Additional support for data protection impact assessments or relations with regulators may be available and would require mutual agreement on fees, the scope of Silverchair's involvement, and any other terms that the Parties deem appropriate.

10. Data Transfers

Silverchair will comply with all Applicable Laws applicable to Silverchair in its role as provider of the Services. Customer will comply with all Applicable Laws relevant to use of the Services, including by obtaining any consents and providing any notices required under Applicable Laws for Silverchair to provide the Services. Customer will ensure that Customer and Customer's authorized users are entitled to transfer the Personal Data to Silverchair so that Silverchair and its Subprocessors may lawfully Process the Personal Data in accordance with this DPA.

Customer authorizes Silverchair and its Subprocessors to make international transfers of the Personal Data in accordance with this DPA so long as Applicable Law for such transfers is respected.

To the extent legally required, (i) the Standard Contractual Clauses apply and take precedence over the rest of this DPA to the extent of any conflict and (ii) by agreeing to this DPA, Customer and Silverchair are deemed to be signing the Standard Contractual Clauses.

11. Audits

Silverchair will make available to Customer all information reasonably necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including inspections, conducted by Customer's independent auditor at its own expense.

12. Return or Destruction

Silverchair will, at Customer's choice, return to Customer and/or destroy all Personal Data after the termination or expiration of Customer's subscription to the relevant Services, except to the extent Applicable Law requires storage of the Personal Data, within (a) 30 days for Personal Data in Silverchair's production environment and (b) 90 days for Personal Data from files created for security, backup, or business continuity purposes. If Silverchair has not received Customer's election within 30 days of such termination or expiration, Silverchair may assume that Customer has selected deletion and reserves the right to delete Personal Data consistent with the foregoing. Certification of deletion under Clause 12 of the Standard Contractual Clauses (if they apply) will be provided only on written request.

13. Additional Provisions for California Personal Information

When processing California Personal Information in accordance with the Services, the Parties acknowledge that Silverchair is a Service Provider. The Parties agree that Silverchair will Process California Personal Information as a Service Provider strictly for the purpose of performing the Services under the Agreement or as otherwise permitted by the CCPA.

ANNEX A – STANDARD CONTRACTUAL CLAUSES

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 personal 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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
 - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (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
Docking clause

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 Subprocessors

- (a) 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 Subprocessors at least 30 business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the Subprocessor(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 Subprocessor 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 Subprocessor 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 Subprocessor 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 Subprocessor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the Subprocessor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the Subprocessor 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 Subprocessor contract and to instruct the Subprocessor 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 Subprocessor 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 Subprocessor) 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 Subprocessor), 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 Subprocessor to avoid its own liability.

Clause 13
Supervision

- (a) 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.
- (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.

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

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. If an EU Member State is required, these Clauses shall be governed by the law of the Republic of Ireland. Addendum 1 shall be in effect where UK GDPR or Swiss DPA is applicable.

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 jurisdiction specified 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.

On behalf of the data exporter:

The entity identified as "Customer" in the DPA.

On behalf of the data importer:

Position: Chief Finance & Administrative Officer

Address: Silverchair Science+Communications LLC, 316 E. Main Street, Suite 300, Charlottesville, VA 22902, USA

Email: dataprivacy@silverchair.com

Other information necessary in order for the contract to be binding (if any): None



Signature

(stamp of organisation)

ANNEX 1 TO STANDARD CONTRACTUAL CLAUSES

DESCRIPTION OF TRANSFER

This Annex forms part of the Standard Contractual Clauses.

Data exporter

The data exporter is Customer, a user of the Services.

Data importer

The data importer is Silverchair Science+Communications LLC, provider of the Services.

Data subjects

Depending on Customer's usage, this could include the exporter's members, users, and potential members and users, as well as individuals in other categories.

Categories of data

The open nature of the Services does not impose a technical restriction on the categories of data Customer may provide. The Personal Data Processed by Silverchair may thus include name, email address, telephone and fax number, title, and other information.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify): The subject matter, nature and purpose of the processing are Silverchair's provision of the Services to Customer. This involves storing personal data, making it available to Customer for modification and transmission, and deleting personal data. The processing takes place from the commencement of the Agreement until deletion of all Personal Data by Silverchair in accordance with the DPA.

ANNEX 2 TO STANDARD CONTRACTUAL CLAUSES

SECURITY MEASURES

This Annex forms part of the Standard Contractual Clauses.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Silverchair shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Details for Silverchair's security measures can be found in its Information Security Addendum (www.silverchair.com/legal/ISA).

ANNEX 3 TO STANDARD CONTRACTUAL CLAUSES

SUBPROCESSORS

This Annex forms part of the Standard Contractual Clauses.

Subprocessors are listed at www.silverchair.com/legal/subprocessors.

ADDENDUM 1 – UK AND SWISS ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

This Addendum amends the Standard Contractual Clauses to the extent necessary so they operate for transfers made by the data exporter to the data importer, to the extent that the UK GDPR or Swiss DPA apply to the data exporter's processing when making that transfer.

The Standard Contractual Clauses shall be amended with the following modifications:

- (a) references to "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR or Swiss DPA (as applicable);
- (b) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the UK GDPR or Swiss DPA (as applicable);
- (c) references to Regulation (EU) 2018/1725 shall be removed;
- (d) references to "EU", "Union" and "Member State" shall be replaced with references to the "UK" or "Switzerland" (as applicable);
- (e) Clause 13(a) and Part C of Annex II are not used and the "competent supervisory authority" shall be the United Kingdom Information Commissioner or Swiss Federal Data Protection Information Commissioner (as applicable);
- (f) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland" (as applicable);
- (g) in Clause 17, the Standard Contractual Clauses shall be governed by the laws of England and Wales or Switzerland (as applicable); and
- (h) to the extent the UK GDPR applies to the processing, Clause 18 shall be replaced to state: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts"; and
- (i) to the extent the Swiss DPA applies to the processing, Clause 18 shall be replaced to state: "Any dispute arising from these Clauses shall be resolved by the competent courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts".