Cribl

Data Processing Addendum

1. Application and Scope.

This data processing addendum ("this DPA") applies to Personal Data transferred to Cribl through or related to your use of Cribl's products or services ("Covered Activities") under Cribl's Standard Terms of Service or other written agreements between you and Cribl that incorporate this DPA by reference ("Applicable Agreement").

Covered Activities include without limitation your use of your access to Cribl's products and services, including without limitation use by persons or organizations that you have authorized to use Cribl's products or services on your behalf, such as your affiliates or subsidiaries. You may only use Cribl's products or services on behalf of others to the extent allowed by an Applicable Agreement.

This DPA supplements Applicable Agreements and includes, to the extent provided by this DPA, Schedule 1 – Standard Contract Clauses: Controller to Processor, and Schedule 2 – Standard Contract Clauses: Controller to Controller, each as may be amended under this DPA. In the event of a conflict between this DPA and an Applicable Agreement, the terms and conditions of this DPA shall control unless specifically superseded by the terms and conditions provided in an Applicable Agreement. In the event of a conflict between this DPA and Schedule 1 or Schedule 2, the applicable schedules shall control to the extent necessary to resolve the conflict.

This DPA is intended to comply with the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 ("the GDPR") and other applicable data protection laws ("Data Protection Laws"), but only to the extent they apply. Words and phrases that are capitalized in this DPA shall have the same meanings as provided in the GDPR as of January 1, 2022, unless otherwise defined in this DPA.

2. Roles and Responsibilities.

You are the Controller for all Personal Data that you submit to Cribl or through Covered Activities ("Customer Personal Data"). Cribl is the Processor for Customer Personal Data. This DPA and all Applicable Agreements are your documented processing instructions.

You and Cribl are each independent Controllers for Personal Data that you submit to Cribl related to the creation, administration, or support of your account with Cribl, including the name, username, email address, and phone number of authorized users of Cribl's products or services and billing contacts ("Account Data"). You are responsible for ensuring Account Data is accurate.

You are responsible for ensuring that you have a sufficient legal basis to send Customer Personal Data and Account Data to Cribl. You are solely responsible for ensuring that no special categories of Personal Data (GDPR Article 9) or Personal Data relating to criminal convictions or offenses (GDPR Article 10) are sent to Cribl.

3. **Processing of Personal Data.**

Cribl shall Process Customer Personal Data as requested through instructions made through Cribl's products or services or otherwise to Cribl. In processing Customer Personal Data, Cribl shall comply with this DPA and all applicable Data Protection Laws.

You cannot send Customer Personal Data or Account Data to Cribl unless you are allowed to do so by applicable law and only then to the extent allowed by applicable law and Cribl's Privacy Policy.

4. **Sub-processors.**

Cribl may use sub-processors listed in Schedule 1 to process Customer Personal Data under this DPA ("Sub-processors"). All Sub-processors shall enter into a written agreement with Cribl related to data protection requirements no less protective of Customer Personal Data than those provided in this DPA.

Cribl may add or replace Sub-processors as it deems appropriate, but in all cases shall remain responsible to you for the provision of products and services as agreed under Applicable Agreements and liable for the acts and omissions of Sub-processors related to Cribl's performance under this DPA to the same extent that Cribl would be liable if it performed such acts or omissions itself.

Cribl will send you a written notice of new or replacement Sub-processors that will process Customer Personal Data ("Change Notice") before such Sub-processors Processes Customer Personal Data. You may object to any new or replacement Sub-processors on reasonable grounds related to the protection of Customer Personal Data by submitting an email to privacy@cribl.io within fourteen days of receiving a Change Notice ("Objection").

Cribl may resolve your Objection to a new or replacement Sub-processor by Processing Customer Personal Data without using that Sub-processor, not using that Sub-processor for any Processing, correcting any issues or other steps identified in your Objection, or not providing (or you not using) the portions of Cribl's products or services that would use that Sub-processor by mutual agreement. Cribl may use the new or replacement Sub-processor during the Objection process.

If your Objection is not resolved to your satisfaction or to Cribl's satisfaction, you or Cribl may terminate the Applicable Agreement. Upon such terminations, you must pay, within thirty days from the date the agreement ended, any unpaid balance owed to Cribl related to your use of Cribl's products or services less the balance attributable to the unused remainder of the contract term or unused paid usage, as applicable. Cribl will refund prior payments attributable to the unused remainder of the contract term or unused paid usage.

If you do not submit an Objection within fourteen days of receiving a Change Notice, you will be deemed to have authorized Cribl to use the new or replacement Sub-processor and waived your right to object to that Sub-processor.

5. **Access.**

Cribl shall take reasonable steps to limit access to Customer Personal Data to only those employees, agents, contractors, and Sub-processors who need to have access to Customer Personal Data to fulfill the purposes of this DPA or an Applicable Agreement, or to comply with Applicable Laws.

Cribl shall ensure that all employees, agents, contractors, and Sub-processors who obtain access to Customer Personal Data under this DPA are subject to confidentiality requirements by a contract between Cribl and each such person.

6. **Security.**

Cribl shall use technical and organizational measures as appropriate to ensure a level of security appropriate to the risks to the rights and freedoms of Data Subjects while considering (1) the state of the art, (2) the costs of implementation, (3) the varying likelihood and severity of risks to the rights and freedoms of natural persons, including risks related to a data breach of Customer Personal Data, and (4) the nature, scope, context, and purposes of Processing ("Security Measures").

Security Measures include without limitation those provided in Annex 2 of Schedule 1 for Customer Personal Data and those provided in Annex 2 of Schedule 2 for Account Data.

Cribl may make from time to time such changes to Security Measures as Cribl determines necessary or appropriate, including without limitation to comply with Applicable Law. No such changes may reduce the level of protection for Customer Personal Data below what is required by this DPA or an Applicable Agreement.

Cribl will take reasonable steps to ensure compliance with Security Measures by its employees, agents, contractors, and Sub-processors to the extent applicable to their respective roles and responsibilities.

7. Data Subject Rights.

Cribl shall notify you, to the extent allowed by Applicable Law, of any request that it receives from a Data Subject related to Customer Personal Data. You are responsible for responding to requests from Data Subjects. Cribl will not respond to requests it receives except to advise Data Subjects to contact you. Cribl may confirm to a Data Subject that the Data Subject's request related to you.

Upon request, Cribl will provide you reasonable assistance to respond to requests to exercise Data Subject rights under Applicable Law Cribl to the extent allowed by Applicable Law for requests made in accordance with Applicable Law and to the extent reasonably possible using Cribl's products and services given the nature of the Customer Personal Data Processed. You shall be responsible for costs related to Cribl's assistance.

8. **Deletion Upon Termination.**

Upon the termination of an Applicable Agreement, Cribl will delete data related to the Applicable Agreement, including Customer Personal Data, from Cribl's products and services to the extent applicable, between thirty and ninety days of the termination of the Applicable Agreement. Notwithstanding the foregoing, Cribl is not obligated to delete data, including Customer Personal Data, to the extent Cribl is required to retain Customer Personal Data by Applicable Law or other applicable legal requirements.

You are responsible for exporting all data, including Customer Personal Data, from Cribl's products and services within thirty days of the termination of the Applicable Agreement.

9. **Data Breaches.**

Cribl will notify you within forty-eight hours of becoming aware of a Data Breach involving Customer Personal Data stored or Processed by Cribl or its Sub-processors ("Customer Personal Data Breach"). Customer Data Breaches do not include Data Breaches caused by you, persons or organizations that you have authorized to use Cribl's products or services on your behalf, or your affiliates or subsidiaries.

Cribl will issue notices of Customer Personal Data Breaches through Cribl's products or services related to the Data Breach, emailing you using the email address you have provided to Cribl for notices or listed on the signature page of an Applicable Agreement, or using the notice procedures provided in the Applicable Agreement. You are responsible for ensuring Cribl has accurate contact information for such notices.

Cribl will take such actions related to Customer Personal Data Breaches and its Security Measures as it deems necessary and appropriate to identify and address the cause or causes of Customer Personal Data Breaches. Cribl will provide you with reasonable cooperation and assistance related to Customer Personal Data Breaches, reasonable information in Cribl's possession related to Customer Personal Data Breaches including without limitation, to the extent allowed by Applicable Law, remediation efforts and notifications to appropriate Supervisory Authorities, and, to the extent known, the possible cause or causes of Customer Personal Data Breaches, the possible categories or Data Subjects and types of Customer Personal Data involved in Personal Data Breaches, and possible consequences to Data Subjects.

Cribl's notification and other actions taken related to Customer Personal Data Breaches are not acknowledgements of fault or liability.

Cribl will not reference you in any public filings, notices, or press releases associated with Customer Personal Data Breaches without your prior consent except to the extent required by Applicable Law.

You will provide Cribl with copies of any proposed notices to a Supervisory Authority, Data Subjects, or the public related to a Customer Personal Data Breach before issuing such notices and, to the extent allowed by Applicable Law, allow Cribl to provide clarifications or corrections to such notices with sufficient time before applicable deadlines.

10. **Audits.**

Cribl will allow you to conduct an audit of Cribl's policies and procedures as may be required to demonstrate Cribl's compliance with this DPA and Applicable Law. You must provide at least thirty days' written notice of such audits and can only conduct one audit during any twelve-month period except as required by a Supervisory Authority or required due to a Customer Personal Data breach.

All audits shall be conducted in a manner that minimizes disruptions to Cribl's normal business operations and protects the confidentiality of information obtained through such audits in accordance with Applicable Agreements. You and Cribl shall mutually agree on each audit's participants, schedule, and scope. Cribl may require persons involved in audits to execute mutually agreeable confidentiality and non-disclosure agreements and all such persons shall comply with this DPA and Cribl's security policies and procedures. Audits do not allow your or any third-party auditor to access Cribl's hosting sites, underlying systems, or infrastructure. You shall reimburse Cribl for time spent by Cribl and its personnel in connection with the audit.

You must provide Cribl with all reports and any identified non-compliance arising from audits conducted under this DPA.

11. **Assistance and Impact Assessments.**

Cribl will, considering the nature, scope, context, and purposes of the Processing, provide reasonable cooperation and assistance as needed for you to comply with your obligations under Applicable Law, including the requirement for you to assess the impact of Processing on the protection of Customer Personal Data ("Impact Assessment for Personal Customer Data") and as required related to your cooperation with a Supervisory Authority under Applicable Law.

Cribl will, considering the nature, scope, context, and purposes of the Processing, assess the impact of Processing on the protection of Account Data for which it is a Controller ("Impact Assessment for Account Data").

12. **Data Transfers.**

You consent to such cross-border transfers of Customer Personal Data and Account Data to Cribl and Cribl's products and services as may be required to the United States or other jurisdiction in

which Customer Personal Data or Account Data may be processed, including without limitation from the European Union or the European Economic Area to the United States.

You agree that the performance of this DPA and all Applicable Agreements requires the transfer of Customer Personal Data and Account Data outside the Union and the European Economic Area, including without limitation transfers from you to Cribl and from Cribl to a Sub-processor.

Schedule 1 and Schedule 2 apply only when Customer Personal Data and Account Data are transferred outside of the EU or the EEA to any country not recognized by the European Commission as having an adequate level of protection under Applicable Law. Schedule 1 relates to data transfers from Controllers to Processors and Schedule 2 relates to data transfers from Controllers to Controllers.

The use of the Standard Contract Clauses in Schedule 1 and Schedule 2, including Cribl's Security Measures, provide appropriate safeguards to protect Customer Personal Data and Account Data transferred under this DPA and Applicable Agreements. The Standard Contract Clauses in Schedule 1 and Schedule 2 have been adopted by the European Commission under Applicable Law.

--

Adopted 2022-02-01.

Schedule 1 – Standard Contract Clauses: Controller to Processor

Annex 1. **Categories of Data Subjects, Types of Customer Personal Data being Processed, and the Nature and Purpose of the Processing.**

Annex 2. **Security Measures.**

Annex 3. **List of Sub-processors.**

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 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) 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 thirty days in advance, 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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(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 Minimization

(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 [for Module Three: and the controller] 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

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, 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 Ireland.

(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.

Schedule 1 – Annex 1

A. LIST OF PARTIES

Data Exporter(s)

1. Name: The entity identified as "you" in this DPA.
   Address: The address provided in this DPA for you.

   Contact person's name, position, and contact details:
   The information provided in this DPA for you.

   Activities relevant to the data transferred under these Clauses:
   You will use Cribl's products and services to use and receive support from Cribl related to Cribl's products and services under Applicable Agreements, allow Cribl and your employees and other users of Cribl's products and services to manage the business relationship between you and Cribl, and provide written instructions to Cribl as appropriate.

   Role (controller/processor): Controller

Data Importer(s):

1. Name: Cribl, Inc.
   Address: 44 Tehama Street, Suite 201, San Francisco, CA 94105

   Contact person's name, position, and contact details:
   Jerry Sharum, VP – Legal, notice@cribl.io.

   Activities relevant to the data transferred under these Clauses:
   Cribl will process Customer Personal Data to provide Cribl's products and services to the data exporter under Applicable Agreements, allow the data exporter's employees and other users of Cribl's products and services to use and receive support from Cribl related to Cribl's products and services, allow Cribl and the data exporter's employees and other users of Cribl's products and services to manage the business relationship between Cribl and the data exporter, perform actions under Applicable Agreements, perform actions as documented by written instructions from the data exporter, and perform actions related to providing, supporting, managing, and improving Cribl's products and services.

   Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

The categories of data subjects whose data constituting Customer Personal Data may be transferred include the data exporter's users, customers, vendors, and end users.

Categories of personal data transferred:
The categories of Customer Personal Data that may be transferred include Customer Personal Data that is sent to Cribl or through Cribl's products and services, including without limitation data processed through Cribl's products and services and the name, position, and contact information of the data exporter's data subjects.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:
No sensitive data is transferred.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):
Customer Personal Data is transferred on a potentially continuous basis when transferred through Cribl's products and services, and on an intermittent or one-time basis when data is transferred related to activities such as receiving support and managing the business relationship between Cribl and the data exporter.

Nature of the processing:
The nature of Cribl's processing includes analysis, filtering, storage, routing, and transmission of data, as well as other services and functionality described in Applicable Agreements, this DPA, and Cribl's documentation at https://docs.cribl.io/.

Purpose(s) of the data transfer and further processing:
The purpose of the data transfer and further processing includes providing, supporting, managing, and improving Cribl's products and services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:
Customer Personal Data will be retained in accordance with the data exporter's configuration of Cribl's products and services or as otherwise provided in Cribl's documentation.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:
The subject matter of the processing by Sub-processors is to aid in providing, supporting, managing, and improving Cribl's products and services, including without limitation the data exporter's use of Cribl's products and services as outlined in the DPA and Applicable Agreements.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:
The competent supervisory authorities are the Data Protection Commission of Ireland except as provided in Clause 13, in which case the competent supervisory authority shall be the supervisory authority provided in Applicable Agreements.

Schedule 1 – Annex 2

Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data

Cribl's Security Measures as of the date of this DPA include without limitation:

1. **System Protections.** Cribl secures its data processing and storage systems with access to Customer Personal Data and Account Data by using access controls, business continuity programs, change management procedures, compliance programs, encryption, secure and high-availability systems, monitoring and testing activities, and its other information security program protections, each as described below, following industry standard practices.

2. **Access Controls.** Cribl uses role-based access controls that limit access to Customer Personal Data and Account Databased on a need to know (or access). Customer Personal Data and Account Data cannot be accessed, modified, or deleted by persons or processes that do not have the authority to do so. Access controls are implemented using single-sign-on and managed access technology to provision and deprovision access on a timely basis whenever a person or system no longer needs to know or access Customer Personal Data or Account Data.

3. **Business Continuity.** Cribl uses documented business continuity plans and procedures to maximize the availability of its data processing and storage systems and respond to disruptions effectively, including business continuity plans specific to Cribl.Cloud and Cribl's support function. Cribl's business continuity plans include the identification of potential disruptions, business impact assessments, mitigation strategies, accepted risks, response procedures, testing, and documentation on the identification and resolution of issues based on testing and other reviews. Cribl's business continuity plans are reviewed and tested at least annually and whenever circumstances require.

4. **Change Management.** Cribl uses documented policies and procedures governing change management related to Cribl.Cloud and Cribl's infrastructure to ensure changes are tested and approved before moving into production.

5. **Compliance.** Cribl uses documented policies and procedures governing Cribl's information security program and reviews those policies and procedures at least annually. Cribl uses documented policies and procedures governing Cribl's risk management program and reviews those policies and procedures at least annually. Cribl follows guidelines for SSAE 18 SOC2 and is in its observation period for attestation. Cribl will provide once per year its most recent SOC2 report upon request.

6. **Encryption.** Cribl uses industry standard encryption to store Customer Personal Data and Account Data at rest and in transit consistent with industry standard practices. Cribl uses documented policies and procedures governing cryptography and key management.

7. **High-availability Services.** Cribl uses high-availability services to provide, support, improve, and manage Cribl's products and services using industry standard security practices.

8. **Monitoring and Testing.** Cribl uses documented policies and procedures governing vulnerability management and network security related to Cribl.Cloud and Cribl's other products and services. Pursuant to these procedures, Cribl undergoes the penetration testing at least annually related to Cribl.Cloud and its other products and services as applicable and vulnerability scanning at least quarterly. Cribl also uses end-point protection and monitoring, managed detection and response services, managed SIEM services, configuration and access logging, and other security monitoring and testing activities. Cribl remediates issues identified in monitoring and testing as appropriate.

9. **Other Information Security Practices.** Cribl uses technical safeguards and other security measures to ensure the security and confidentiality of Customer Personal Data. Cribl logically separates Customer Personal Data from other customer's Personal Data and separates its production environment from its testing and development environment.

Schedule 1 – Annex 3

List of Sub-processors

Cribl's list of Sub-processors as of the date of this DPA include the Sub-processors listed below. You as the Controller and data exporter have approved the use of these Sub-processors. Cribl may add or replace Sub-processors as described in Clause 9. Cribl's current list of Sub-processors is available at https://cribl.io/legal/subprocessors.

Amazon Web Services hosts Cribl.Cloud and processes Customer Personal Data related to Cribl.Cloud and Cribl's other products and services.

Atlassian Pty Ltd (Jira) hosts Cribl's issue-tracking system related to providing, supporting, managing, and improving Cribl's products and services.

Google hosts Cribl's email and office software applications used to communicate with customers, potential customers, partners, and other individuals.

Marketo manages the collection of cookies and other information used in Cribl's products and services and processes Customer Personal Data from information collected through Cribl's products and services.

Intercom provides communication functionality in Cribl's products and services, and processes Customer Personal Data related to Cribl's business relationships and customer support activities.

Looker provides analytical services and processes Customer Personal Data related to Cribl's analytics activities.

Metronome provides billing services and processes Customer Personal Data related to Cribl's products and services.

OneTrust provides privacy, security, and governance services, including the detection of all first- and third-party cookies and the consent provided to use cookies.

Outreach provides customer management services, processes Customer Personal Data related to Cribl's business relationships, and integrates with SalesForce.

SalesForce provides customer management services and processes Customer Personal Data related to Cribl's business relationships and customer support activities.

Segment provides integration services that connects customer data across different data sources and is used to manage Cribl's business relationships and analytics activities.

Slack provides customer support and communication services and processes Customer Personal Data related to Cribl's business relationships and customer support activities.

Snowflake provides data storage and is used for Cribl's analytics activities and processes Customer Personal Data related to Cribl's business relationships and customer support activities.

Zoom provides webinar and meeting services and processes Customer Personal Data related to Cribl's business relationships and customer support activities.

Schedule 2 – Standard Contract Clauses: Controller to Controller

Annex 1. **Categories of Data Subjects, Types of Customer Personal Data being Processed, and the Nature and Purpose of the Processing.**

Annex 2. **Security Measures.**

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.

(d) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(e) 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 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and Data Minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage Limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.4 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they 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 subject. 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.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the

personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward Transfers

The data importer shall not disclose the personal data 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") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it 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 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the Authority of the Data Importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and Compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9
Use of Sub-processors

Inapplicable

Clause 10
Data Subject Rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge :

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

(e) The data importer may not invoke the conduct of a processor or 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 Minimization

(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 [for Module Three: and the controller] 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

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows 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 Ireland.

(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.

Schedule 2 – Annex 1

A. LIST OF PARTIES

Data Exporter(s)

1. Name: The entity identified as "you" in this DPA.
   Address: The address provided in this DPA for you.

   Contact person's name, position, and contact details:
   The information provided in this DPA for you.

   Activities relevant to the data transferred under these Clauses:
   You will process Account Data related to receiving Cribl's products and services, allowing you and your employees and other users of Cribl's products and services to use and receive support from Cribl related to Cribl's products and services, allow Cribl and your employees and other users to manage the business relationship between you and Cribl, and perform actions under Applicable Agreements.

   Role (controller/processor): Controller

Data Importer(s):

2. Name: Cribl, Inc.
   Address: 44 Tehama Street, Suite 201, San Francisco, CA 94105

   Contact person's name, position, and contact details:
   Jerry Sharum, VP – Legal, notice@cribl.io.

   Activities relevant to the data transferred under these Clauses:
   Cribl will process Account Data to provide Cribl's products and services to you under Applicable Agreements, allow your employees and other users of Cribl's products and services to use and receive support from Cribl related to Cribl's products and services, allow Cribl and your employees and other users of Cribl's products and services to manage the business relationship between you and Cribl, perform actions under Applicable Agreements, and perform actions related to providing, supporting, managing, and improving Cribl's products and services.

   Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

The categories of data subjects whose data constituting Account Data may be transferred include the data exporter's users.

Categories of personal data transferred:
The categories of Account Data that may be transferred include Account Data that is sent to Cribl or through Cribl's products and services, including without limitation data processed through Cribl's products and services and the name, position, and contact information of the data exporter's data subjects.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:
No sensitive data is transferred.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):
Account Data is transferred on a potentially continuous basis when transferred through Cribl's products and services, and on an intermittent or one-time basis when data is transferred related to activities such as receiving support and managing the business relationship between Cribl and the data exporter.

Nature of the processing:
The nature of Cribl's processing includes account management and other activities described in Cribl's Privacy Policy, which is available at https://cribl.io/privacy-policy/.

Purpose(s) of the data transfer and further processing:
The purpose of the data transfer and further processing includes providing, supporting, managing, and improving Cribl's products and services through providing Cribl's products and services, supporting Cribl's products and services, calculating fees, communicating with the data exporter and its data subjects, and otherwise managing the data exporter's account.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:
Cribl retains Account Data for only as long as necessary to manage the data exporters account pursuant applicable data retention requirements, including as described in Cribl's Data Retention Policy and Privacy Policy, which is available at https://cribl.io/privacy-policy/.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:
The subject matter of the processing by Sub-processors is to aid in providing, supporting, managing, and improving Cribl's products and services, including without limitation the data exporter's use of Cribl's products and services as outlined in the DPA and Applicable Agreements.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:
The competent supervisory authorities are the Data Protection Commission of Ireland except as provided in Clause 13, in which case the competent supervisory authority shall be the supervisory authority provided in Applicable Agreements.

Schedule 2 – Annex 2

Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data

Cribl's Security Measures as of the date of this DPA include without limitation:

1. **System Protections.** Cribl secures its data processing and storage systems with access to Customer Personal Data and Account Data by using access controls, business continuity programs, change management procedures, compliance programs, encryption, secure and high-availability systems, monitoring and testing activities, and its other information security program protections, each as described below, following industry standard practices.

2. **Access Controls.** Cribl uses role-based access controls that limit access to Customer Personal Data and Account Databased on a need to know (or access). Customer Personal Data and Account Data cannot be accessed, modified, or deleted by persons or processes that do not have the authority to do so. Access controls are implemented using single-sign-on and managed access technology to provision and deprovision access on a timely basis whenever a person or system no longer needs to know or access Customer Personal Data or Account Data.

3. **Business Continuity.** Cribl uses documented business continuity plans and procedures to maximize the availability of its data processing and storage systems and respond to disruptions effectively, including business continuity plans specific to Cribl.Cloud and Cribl's support function. Cribl's business continuity plans include the identification of potential disruptions, business impact assessments, mitigation strategies, accepted risks, response procedures, testing, and documentation on the identification and resolution of issues based on testing and other reviews. Cribl's business continuity plans are reviewed and tested at least annually and whenever circumstances require.

4. **Change Management.** Cribl uses documented policies and procedures governing change management related to Cribl.Cloud and Cribl's infrastructure to ensure changes are tested and approved before moving into production.

5. **Compliance.** Cribl uses documented policies and procedures governing Cribl's information security program and reviews those policies and procedures at least annually. Cribl uses documented policies and procedures governing Cribl's risk management program and reviews those policies and procedures at least annually. Cribl follows guidelines for SSAE 18 SOC2 and is in its observation period for attestation. Cribl will provide once per year its most recent SOC2 report upon request.

6. **Encryption.** Cribl uses industry standard encryption to store Customer Personal Data and Account Data at rest and in transit consistent with industry standard practices. Cribl uses documented policies and procedures governing cryptography and key management.

7. **High-availability Services.** Cribl uses high-availability services to provide, support, improve, and manage Cribl's products and services using industry standard security practices.

8. **Monitoring and Testing.** Cribl uses documented policies and procedures governing vulnerability management and network security related to Cribl.Cloud and Cribl's other products and services. Pursuant to these procedures, Cribl undergoes the penetration testing at least annually related to Cribl.Cloud and its other products and services as applicable and vulnerability scanning at least quarterly. Cribl also uses end-point protection and monitoring, managed detection and response services, managed SIEM services, configuration and access logging, and other security monitoring and testing activities. Cribl remediates issues identified in monitoring and testing as appropriate.

9. **Other Information Security Practices.** Cribl uses technical safeguards and other security measures to ensure the security and confidentiality of Customer Personal Data. Cribl logically separates Customer Personal Data from other customer's Personal Data and separates its production environment from its testing and development environment.