Data Processing Addendum

These personal information processing terms and schedules constitute Searchie's data processing addendum ("DPA") and are included by reference to the Software as a Service Subscription Agreement between Searchie and Customer (the "Agreement"). In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

Searchie reserves the right to update the contents of this DPA from time to time upon notice to Customer by posting a notice to its website.

The term of this DPA will follow the term of the Agreement. Capitalized words not otherwise defined in this DPA will have the meaning as set forth in the Agreement.

Article 1. Interpretation

Section 1.01 Definitions

(a) "California Personal Information" means Personal Information that is subject to the protection of the CCPA.

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

(c) "Consumer", "Business", "Sell" and "Service Provider" will have the meanings given to them in the CCPA.

(d) "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.

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European Data Protection Laws, the CCPA and the data protection and privacy laws of Canada; in each case as amended, repealed, consolidated or replaced from time to time.

(f) "Data Subject" means the individual to whom Personal Information relates.

(g) "Deletion Date" means the date on which data is to be deleted as set out from time to time in Searchie's data retention policy available here .

(h) "Europe" means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

(i) "European Data" means Personal Information that is subject to the protection of European Data Protection Laws.

(j) "European Data Protection Laws" means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Information and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of Personal Information and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss DPA"); in each case, as may be amended, superseded or replaced.

(k) “Instructions” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Information (including, but not limited to, depersonalizing, blocking, deletion, making available).

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

(m) “Personal Information Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed by Searchie and/or Searchie’s Sub-Processors in connection with the provision of the Services. "Personal Information Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Information, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

(n) “Personal Information Consent” means the personal information consent used by Searchie from time to time, available here.

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

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

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

(r) “Sub-Processor” means any Processor engaged by Searchie to assist in fulfilling Searchie’s obligations with respect to the provision of the Services under the Agreement. Sub-Processors may include third parties but will exclude any Searchie employee or consultant.

Article 2. Customer Responsibilities

Section 2.01 Compliance with Laws.

Within the scope of the Agreement and in its use of the services, Customer will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Information and the Instructions it issues to Searchie.

In particular but without prejudice to the generality of the foregoing, Customer acknowledges and agrees that it will be solely responsible for: (i) the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Personal Information; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Information, including obtaining any necessary consents and authorizations (particularly for use by

Customer for marketing purposes); (iii) ensuring Customer has the right to transfer, or provide access to, the Personal Information to Searchie for Processing in accordance with the terms of the Agreement (including this DPA); (iv) ensuring that Customer Instructions to Searchie regarding the Processing of Personal Information comply with applicable Laws, including Data Protection Laws; and (v) complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Services, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices. Customer will inform Searchie without undue delay if Customer are not able to comply with Customer responsibilities under this 'Compliance with Laws' section or applicable Data Protection Laws.

Section 2.02 Personal Information Consent.

Customer will only collect, use, disclose and retain Personal Information according to the terms of the Personal Information Consent and in no event in an unreasonable way.

SEARCHIE DOES NOT WARRANT THAT OBTAINING CONSENT FOR THE PROCESSING OF PERSONAL INFORMATION IN THE FORM PROVIDED BY THE PERSONAL INFORMATION CONSENT WILL SATISFY THE DATA PROTECTION LAWS APPLICABLE TO CUSTOMER AND/OR ITS AUTHORIZED USERS.

Section 2.03 Customer Instructions.

The Parties agree that the Agreement (including this DPA), together with Customer's use of the Services in accordance with the Agreement, constitute Customer's complete Instructions to Searchie in relation to the Processing of Personal Information, so long as Customer may provide additional instructions during the Service Period that are consistent with the Agreement, the nature and lawful use of the Services.

Section 2.04 Security.

Customer is responsible for independently determining whether the data security provided under the Agreement adequately meets Customer obligations under applicable Data Protection Laws.

Article 3. Searchie Obligations

Section 3.01 Compliance with Instructions.

Searchie will only Process Personal Information for the purposes described in this DPA or as otherwise agreed within the scope of Customer's lawful Instructions, except where and to the extent otherwise required by applicable Law. Searchie is not responsible for compliance with any Data Protection Laws applicable to Customer or Customer industry that are not generally applicable to Searchie.

Section 3.02 Conflict of Laws.

If Searchie becomes aware that it cannot Process Personal Information in accordance with Customer's Instructions due to a legal requirement under any applicable Law, Searchie will (i) promptly notify Customer of that legal requirement to the extent permitted by the applicable Law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Information) until such time as Customer issues new Instructions with which Searchie is able to comply. If this provision is invoked, Searchie will not be liable to Customer under the Agreement for any failure to perform the applicable Services until such time as Customer issues new lawful Instructions with regard to the Processing.

Section 3.03 Security.

Searchie will implement and maintain appropriate technical and organizational measures to protect Personal Information from Personal Information Breaches as described in Searchie's security policy as amended from time to time, a current copy of which is available here (the "Security Policy"). Notwithstanding any provision to the contrary, Searchie may modify or update the Security Policy at Searchie's discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Policy.

Section 3.04 Confidentiality.

Searchie will ensure that any personnel whom Searchie authorizes to Process Personal Information on Searchie's behalf are subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Information.

Section 3.05 Personal Information Breaches.

Searchie will notify Customer without undue delay after Searchie becomes aware of any Personal Information Breach and will provide timely information relating to the Personal Information Breach as it becomes known or reasonably requested by Customer. At Customer's request, Searchie will promptly provide Customer with such reasonable assistance as necessary to enable Customer to notify relevant Personal Information Breaches to competent authorities and/or affected Data Subjects, if Customer is required to do so under Data Protection Laws.

Section 3.06 Deletion of Customer Data and Personal Information.

Searchie will securely delete all Customer Data by the Deletion Date, including Customer's Confidential Information and Personal Information Processed pursuant to this DPA, provided that, for clarity, Searchie may retain Resultant Data.

Article 4. Data Subject Requests

(a) The Services provide Customer with a number of controls that Customer can use to retrieve, correct, delete or restrict Personal Information which Customer can use to assist it in connection with its obligations under Data Protection Laws, including Customer's obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").

(b) To the extent that Customer is unable to independently address a Data Subject Request through the Services, then upon Customer's written request, Searchie will provide reasonable assistance to Customer to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Information under the Agreement. Customer shall reimburse Searchie for the commercially reasonable costs arising from this assistance.

(c) If a Data Subject Request or other communication regarding the Processing of Personal Information under the Agreement is made directly to Searchie, Searchie will promptly inform Customer and will advise the Data Subject to submit their request to Customer. Customer will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Information.

Article 5. Sub-Processors

(a) Customer agrees that Searchie may engage Sub-Processors to Process Personal Information on its behalf. Searchie has currently appointed, as Sub-Processors, the third parties listed in Schedule B to this DPA. Searchie will notify Customer if Searchie adds or replaces any Sub-Processors listed in Schedule B at least 7 days prior to any such changes.

(b) Where Searchie engages Sub-Processors, Searchie will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Information as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. Searchie will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause Searchie to breach any of its obligations under this DPA.

Article 6. Data Transfers

Customer acknowledges and agrees that Searchie may access and Process Personal Information on a global basis as necessary to provide the Services in accordance with the Agreement, and in particular that Personal Information may be transferred to and Processed by Searchie in Canada, the United States and other jurisdictions where Searchie and its Sub-Processors have operations. Wherever Personal Information is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

Article 7. Additional Provisions for European Data

Section 7.01 Scope.

This 'Additional Provisions for European Data' article shall apply only with respect to European Data.

Section 7.02 Roles of the Parties.

When Processing European Data in accordance with Customer Instructions, the parties acknowledge and agree that Customer is the Controller of European Data and Searchie is the Processor. Customer will provide Searchie with prior notice identifying the relevant Personal Information before transferring European Data to Searchie.

Section 7.03 Instructions.

If Searchie believes that a Customer Instruction infringes European Data Protection Laws (where applicable), Searchie will inform Customer without delay.

Section 7.04 Objection to New Sub-Processors.

Searchie will give Customer the opportunity to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Personal Information within 7 days of notifying Customer in accordance with the ‘Sub-Processors’ section. If Customer does notify Searchie of such an objection, the Parties will discuss Customer’s concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Searchie will, at Searchie’s sole discretion, either not appoint the new Sub-Processor, or permit Customer to suspend or terminate the affected Services in accordance with the termination provisions of the Agreement without liability to either Party (but without prejudice to any fees incurred by Customer prior to suspension or termination). The Parties agree that by complying with this Section 7.04, Searchie fulfils its obligations under Clause 9 of the Standard Contractual Clauses.

Section 7.05 Sub-Processor Agreements.

For the purposes of Clause 9(c) of the Standard Contractual Clauses, Customer acknowledges that Searchie may be restricted from disclosing Sub-Processor agreements but that Searchie shall use reasonable efforts to require any Sub-Processor Searchie appoints to permit it to disclose the Sub-Processor agreement to Customer and shall provide (on a confidential basis) all information Searchie reasonably can.

Section 7.06 Data Protection Impact Assessments and Consultation with Supervisory Authorities.

To the extent that the required information is reasonably available to Searchie, and Customer does not otherwise have access to the required information, Searchie will provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by European Data Protection Laws.

Section 7.07 Transfer Mechanisms for Data Transfers.

(a) Searchie shall not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Information (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Information, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.

(b) Customer acknowledges that in connection with the performance of the Services, Searchie is a recipient of European Data in Canada. The parties acknowledge that Canada has been recognized as providing adequate protection by the relevant authorities to permit the transfer of European Data without further transfer mechanisms.

(c) The parties agree that for the purposes of the Standard Contractual Clauses, (i) Searchie will be the "data importer" and Customer will be the "data exporter"; (ii) the Exhibits of the Standard Contractual Clauses shall be populated with the relevant information set out in Schedule A and Schedule B of this DPA; and (iii) if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

(d) To the extent that and for so long as the Standard Contractual Clauses as implemented in accordance with this DPA cannot be relied on by the parties to lawfully transfer Personal Information in compliance with the UK GDPR, the applicable standard data protection clauses issued, adopted or permitted under the UK GDPR shall be incorporated by reference, and the Annexes, appendices or tables of such clauses shall be deemed populated with the relevant information set out in Schedule A and Schedule B of this DPA.

(e) If for any reason Searchie cannot comply with its obligations under the Standard Contractual Clauses or is breach of any warranties under the Standard Contractual Clauses, and Customer intends to suspend the transfer of European Data to Searchie or terminate the Standard Contractual Clauses, Customer agrees to provide Searchie with reasonable notice to enable Searchie to cure such non-compliance and reasonably cooperate with Searchie to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If Searchie has not or cannot cure the non-compliance, Customer may suspend or terminate the affected part of the Services in accordance with the Agreement without liability to either party (but without prejudice to any fees Customer has incurred prior to such suspension or termination).

Section 7.08 Demonstration of Compliance.

Searchie will make all information reasonably necessary to demonstrate compliance with this DPA available to Customer and allow for and contribute to audits, including inspections conducted by Customer auditor in order to assess compliance with this DPA. Customer acknowledges and agrees that Customer will exercise its audit rights under this DPA and Clause 8.9 of the Standard Contractual Clauses by instructing Searchie to comply with the audit measures described in this Section 7.08. Customer acknowledges that the Services are hosted by Searchie’s hosting Sub-Processors who maintain independently validated security programs and may not be responsive to Searchie’s requests for information. At Customer written request, Searchie will provide written responses (on a confidential basis) to all reasonable requests for information made by Customer necessary to confirm Searchie’s compliance with this DPA, provided that Customer will not exercise this right more than once per calendar year unless Customer has reasonable grounds to suspect non-compliance with the DPA.

Article 8. Additional Provisions for California Personal Information

Section 8.01 Scope.

The 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information.

Section 8.02 Roles of the Parties.

When processing California Personal Information in accordance with Customer Instructions, the parties acknowledge and agree that Customer is a Business and Searchie is a Service Provider for the purposes of the CCPA. Customer will provide Searchie with prior notice identifying the relevant Personal Information before transferring California Personal Information to Searchie.

Section 8.03 Responsibilities.

The parties agree that Searchie will Process California Personal Information as a Service Provider strictly for the purpose of performing the Services under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA.

Article 9. General Provisions

Section 9.01 Amendments.

Notwithstanding anything else to the contrary in the Agreement and without prejudice to the ‘Compliance with Instructions’ or ‘Security’ sections of this DPA, Searchie reserves the right to make any updates and changes to this DPA.

Section 9.02 Limitation of Liability.

Each Party’s liability, taken in aggregate, arising out of or related to this DPA (and any other DPAs between the Parties) and the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the 'Limitation of Liability' section of the Agreement and any reference in such section to the liability of a Party means aggregate liability of that Party (including under this DPA). In no event shall either party's liability be limited with respect to any individual's data protection rights under this DPA (including the Standard Contractual Clauses) or otherwise.

Schedule A
Details of Processing

Categories of data subjects whose personal information is transferred

- End users of Searchie's content delivery platform (the "Platform") that have been authorized to access the Platform by the Customer and who for greater certainty are:
  - Customer him/herself (if a natural person), Customer's administrators (who may be employees or agents of Customer); and
  - Customer's audience members.

Categories of personal information transferred

Typical:

- Identifying (name, username, unique identifiers, etc.)
- Authenticating (passwords, PINs, etc.)
- Tracking (computer device, contact information, location, etc.)
- Redacted payment information (last 4 digits of credit card, expiry month and expiry year, card type)

Additionally, at Customer's discretion:

- Professional (job titles, salaries, work history, etc.)
- Family (family structure, marriages, divorces, relationships, etc.)
- Demographic (age ranges, physical traits, income brackets, geographic, etc.)
- Such other research data points as may be interesting to Customer that are not sensitive.

NO Sensitive personal information is to be requested by Customer.

The frequency of the transfer

- Continuous

Nature of the processing

- Collection, documentation, organization, structuring, storage, adaptation and modification, making inquiries, reading, use, disclosure by making available, reconciliation or connection, restriction or deletion.

Purpose of the data transfer and further processing

- To fulfill Searchie's contractual obligation to Customer for access and use of the Platform as follows:
  a. authentication purposes;
  b. to create an account profile for the user;
  c. to communicate with the user;
  d. to bill the user, either directly or on behalf of the Customer; and
  e. to improve the quality of Searchie's services.

The period for which the personal information will be retained

- For the duration set out in Searchie's Data Retention Policy here, except that Searchie and its sub-processors may retain personal data as required by applicable law or in their backups, archives, and disaster recovery systems until such personal data is deleted in the ordinary course.

For transfers to sub-processors, the subject matter, nature and duration of the processing

- Sub-processors who host the Platform on their servers will store personal for the purpose of storing it and making it accessible to Searchie, Customer and end users. The duration of processing will be coextensive with Searchie's obligation to operate the Platform (subject the retention provisions above)
- Sub-processors who deliver plug-in features (such as video / audio recording), will process personal data as necessary and only for so long as required to make such plug-in features operate correctly.
- Sub-processors

Schedule B
List of Sub-Processors

(a) Hubspot CRM/Marketing tool

(b) Google analytics

(c) Mailgun

(d) Bitbucket Version Control

(e) Amazon S3 (AWS)

(f) Stripe

(g) Chargebee

(h) Spiffy

Schedule C
Standard Contractual Clauses

Section I - GENERAL

Clause 1. Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Exhibit 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 Exhibit 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 Exhibit I.B.

(d) The Appendix to these Clauses containing the Exhibits 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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4. Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

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

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6. Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Exhibit 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 Exhibit I.A.

(b) Once it has completed the Appendix and signed Exhibit

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 Exhibit 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 Exhibit 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 Exhibit II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Exhibit 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 Exhibit 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 Exhibit 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 7 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 Exhibit II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11. **Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12. **Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13. **Supervision**

(a) Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer 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, 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, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

Section III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14. Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15. Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Section IV - FINAL PROVISIONS

Clause 16. **Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17. **Governing law**

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.

Appendix to Schedule C

EXHIBIT I

A. LIST OF PARTIES

Data exporter is “Customer” as defined in the software as a service subscription agreement between the data exporter and the data importer (the “Software as a Service Subscription Agreement”). The Customer is the controller. Customer’s particulars and contact information are as set out in the order form made under the Software as a Service Subscription Agreement.

Data importer is Searchie. Searchie is the processor. Searchie’s particulars and contact information are as set out in the Software as a Service Subscription Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- End users of Searchie’s online qualitative research platform (the “Community”) that have been authorized to access the Community by the Customer and who for greater certainty are:
  - Customer’s administrators (who may be employees or agents of Customer); and
  - Customer’s research subjects.

Categories of personal data transferred

Typical:

- Identifying (name, username, unique identifiers, etc.)
- Authenticating (passwords, PINs, etc.)
- Preferences / Interests (opinions, interests, dislikes, etc.)
- Tracking (computer device, contact information, location, etc.)

Additionally, at Customer’s discretion:

- Professional (job titles, salaries, work history, etc.)
- Family (family structure, marriages, divorces, relationships, etc.)
- Demographic (age ranges, physical traits, income brackets, geographic, etc.)
- Such other research data points as may be interesting to Customer that are not sensitive.

Sensitive (ONLY TO BE EXPORTED TO SEARCHIE WITH SEARCHIE’S PRIOR WRITTEN CONSENT):

- Medical and Health (physical and mental health, disabilities, etc.)
- Sexual (sex life, sexual orientation, etc.)
- Race (race, ethnic origin, etc.)
- Political (political opinions)

The frequency of the transfer

- Continuous

Nature of the processing

- As necessary to operate the Community and achieve the Customer’s research objectives which for greater certainty means:
  - Migration, setup and hosting personal data as part of the Community;
  - Retrieval and transmission to Authorized Users, Customer and Sub-processors;
  - Encryption, anonymizing, pseudonymizing and compiling;
  - Processing as necessary to facilitate specific product features (such as video / audio recording)

Purpose(s) of the data transfer and further processing

- To fulfill Searchie’s contractual obligation to Customer for access and use of the Community.

The period for which the personal data will be retained

- From the Admin Access Start Date to the Deletion Date, except that Searchie and its sub-processors may retain personal data as required by applicable law or in their backups, archives, and disaster recovery systems until such personal data is deleted in the ordinary course.

For transfers to sub-processors, also specify subject matter, nature and duration of the processing

- Sub-processors who host the Community on their servers will store personal data integrated in the Community for the purpose of storing it and making it accessible to Searchie, Customer and end users. The duration of processing will be coextensive with Searchie’s obligation to operate the Community (subject the retention provisions above)
- Sub-processors who deliver plug-in features (such as video / audio recording), will process personal data as necessary and only for so long as required to make such plug-in features operate correctly.
- Sub-processors who provide technical support will access personal data only as an ancillary consequence of their access to the Community for the purpose of providing technical support services. They will have access to personal data only for the duration of their provision of technical support services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Unless where otherwise required by law, the competent supervisory authority will be the Data Protection Commission of Ireland.

EXHIBIT II
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Please see the Searchie Information Security Policy here