smarsh™
Capture. Reveal. Respond.

Data Processing Addendum

This Data Processing Addendum (this "DPA") forms part of the Smarsh Service Agreement found at www.smarsh.com/legal, unless Client has entered into a different form of subscription agreement with Smarsh, Inc. ("Smarsh") for Smarsh archiving services and, in which case this DPA forms a part of such written agreement (in either case, the "Agreement"). By signing this DPA, Client enters into this Agreement on behalf of itself and, to the extent required under applicable Data Protection Laws, on behalf of its Controller Affiliates (defined below). For the purposes of this DPA only, and except where indicated otherwise, the term "Client" shall include Client and Controller Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services under the Agreement, Smarsh may Process Personal Data on behalf of Client. The parties agree to comply with the terms and conditions of this DPA in connection with Smarsh's Processing of Personal Data. This DPA is an addendum to the Agreement and applies solely to Smarsh's processing of personally identifiable information of individuals in the European Union. To the extent there is a direct conflict between the Agreement and this DPA, this DPA will apply solely with respect to the directly conflicting term. In the event of any conflict between the body of this DPA and any of its Exhibits (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Exhibit B, the Standard Contractual Clauses will prevail.

How to Execute this DPA

1) This DPA consists of two parts: the main body of the Amendment, and Exhibits A and B.

2) This DPA has been pre-signed by Smarsh. The Standard Contractual Clauses in Exhibit B have been pre-signed by Smarsh as the data processor.

3) To complete this DPA, Client must:

    a) Complete the information in the signature box and sign on pages 6, 13, 14, and 15.

    b) Complete the information as the data exporter on Page 2.

Smarsh Inc:	**Client:**
Signature: Tricia Juettemeyer (Sep 20, 2018) Name: Tricia Juettemeyer Title: Assistant General Counsel Date Signed: Sep 20, 2018	Signature: Name: ____________________ Title: ____________________ Date Signed: ____________________
Address: 851 SW 6th Ave. Ste. 800 Portland OR 97204	Address:
DPO/Contact for data protection enquiries legal@smarsh.com	DPO/Contact for data protection enquiries Name/Role: ____________________ Email: ____________________

Name of the data exporting organisation:...

Address: ....

Tel.:..; fax:... ; e-mail: ....

Other information needed to identify the organisation:

....
(the data exporter)

And

Name of the data importing organisation: Smarsh, Inc.

Address: 851 SW 6th Ave. Suite 800 Portland, OR 97204

Tel.: 1-866-SMARSH-1; fax: (971) 998-9967; e-mail: legal@smarsh.com

Other information needed to identify the organisation:

……………………………………………………………………
(the data importer)

[This Space Intentionally Left Blank]

DATA PROCESSING TERMS

1. Definitions. Capitalized terms used in this DPA will have the following meanings:

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with Client. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Controller" means the entity who determines the purposes and means of the Processing of Personal Data.

"Controller Affiliate" means any of Client's Affiliate(s) (a) (i) who are subject to applicable Data Protection Laws of the European Union, the European Economic Area and/or their member states, and/or the United Kingdom, and (ii) permitted to use the Services pursuant to the Agreement between Client and Smarsh, (b) if and to the extent Smarsh processes Personal Data for which such Affiliate(s) qualify as the Controller.

"Client Data" means data received by Smarsh pursuant to the Services from individuals located in the European Union

"Data Protection Laws and Regulations" means the applicable laws and regulations of the European Union, the European Economic Area and their member states, and the United Kingdom regarding the Processing of Personal Data.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"GDPR" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information relating to any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Standard Contractual Clauses" means the agreement executed by and between Client and Smarsh, Inc. and Smarsh Affiliates and attached hereto as Exhibit B pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"Sub-processor" means any Processor engaged by Smarsh to Process Client Data.

"Supervisory Authority" means an independent public authority, which is established by an EU Member State pursuant to Article 51 of the GDPR.

2. Processing of Personal Data.

2.1. Role of the Parties. For purposes of this DPA, with respect to Client Data, Client is the Controller and Smarsh is the Processor. Smarsh or its Affiliates will only engage Sub-processors pursuant to the requirements set forth in Section 4 "Sub-processors" below.

2.2. Client's Processing of Personal Data. Client will only use the Services to Process Personal Data in accordance with Data Protection Laws and Regulations. Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data.

2.3. **Smarsh's Processing of Personal Data.** Smarsh will treat Personal Data as Confidential Information and will only Process Personal Data for the following purposes: (i) Processing as necessary to provide the Services and in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; (iii) Processing to comply with other documented reasonable instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement; (iv) Processing to support or troubleshoot the Services; and (v) Processing for the purpose of enabling Sub-Processors in accordance with Section 4 below.

2.4. **Client Processing Instructions.** Client appoints Smarsh as a Processor to process Client Data on behalf of, and in accordance with, Client instructions and as specified in this DPA, in the Agreement, or as otherwise instructed by Client. Client is responsible for ensuring that its instructions comply with all applicable laws or regulations that apply to Client, including the GDPR and Data Protection Laws and Regulations. In addition to the instructions included in the Agreement, elsewhere in this DPA, or the other instructions provided by Client to Smarsh, the following are deemed instructions by the Client to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing requested or initiated by Users in their use of the Services; and (c) Processing to comply with other reasonable instructions provided by Client (e.g., via email or support tickets).

2.5. **Details of Processing.** The subject-matter of Processing of Personal Data by Smarsh, the duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects processed under this DPA are further specified in Exhibit A (Description of Processing Activities) to this DPA.

3. Rights of Data Subjects.

3.1. **Data Subject Requests.** Smarsh will, to the extent legally permitted, promptly notify Client if Smarsh receives a request from a Data Subject to exercise the following Data Subject rights: access, rectification, restriction of Processing, erasure ("right to be forgotten"), or objection to the Processing (each, a "**Data Subject Request**"). Smarsh will not respond to a Data Subject Request without Client's prior written consent, except that Smarsh may respond to such Data Subject to confirm that the request relates to Client. To the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, Smarsh may, upon Client's request, provide commercially reasonable assistance to facilitate such Data Subject Request, to the extent Smarsh is legally permitted to do so and provided that such Data Subject Request is exercised in accordance with Data Protection Laws and Regulations. To the extent legally permitted, Client will be responsible for any costs arising from Smarsh's provision of such assistance.

4. Sub-Processors.

4.1. **Appointment of Sub-processors.** Client agrees that (a) Smarsh's Affiliates may be retained as Sub-processors; and (b) Smarsh and Smarsh's Affiliates, respectively, may engage third-party Sub-processors in connection with the provision of the Services so long as Smarsh or the Smarsh Affiliate have entered into a written agreement with each Sub-processor containing data protection obligations with respect to the protection of Client Data to the extent applicable to the nature of the services provided to Client by such Sub-processor.

4.2. **List of Current Sub-processors and Notification of New Sub-processors.** Smarsh will provide the current list of Sub-processors for the Services, including the identities of the Sub-processors and their country of location ("**Sub-processor Lists**"). The Sub-processor Lists will be available at www.smarsh.com/legal. Smarsh will provide Client with notification of new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

4.3. **Objection Right for New Sub-processors.** Client may object to Smarsh's use of a new Sub-processor, if Client reasonably believes that making Personal Data available to the Sub-processor violates applicable Data Protection Law, by notifying Smarsh in writing within ten (10) business days after Smarsh's notice of new Sub-Processor under Section 4.2. Client's notice must explain the reasonable grounds for the objection. Smarsh will use commercially reasonable efforts to make available to Client a change in the Services to avoid Processing of Personal Data by the objected-to new Sub-processor. If Smarsh is unable to make available such change, either party may terminate the applicable Order Form(s) with respect only to those Services affected by the use of such new Sub-processor.

4.4. **Liability.** Smarsh will be liable for the acts and omissions of its Sub-processors to the same extent Smarsh would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

5. Security.

5.1. Controls for the Protection of Client Data. Smarsh will maintain appropriate technical and organizational measures, which are designed to protect the security, confidentiality and integrity of Client Data (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Client Data), including as appropriate:

5.1.1. the encryption of Personal Data;

5.1.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.1.3. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

5.1.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing.

5.2. Third-Party Certifications and Audits. Upon Client's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Smarsh will make available to Client a copy or attestation letter of Smarsh's then most recent third-party audits or certifications, as applicable. Upon Client's request, Smarsh shall:

5.2.1. make available, at no cost to Client all information and records reasonably necessary to demonstrate compliance with the obligations set out in this DPA, in the form of Smarsh's standard GDPR information sheet or Smarsh's standard information gathering documentation ("SIG") for information security.

5.2.2. To the extent required by Data Protection Laws and Regulations, allow for and contribute to additional reasonable audits beyond the information provided in the GDPR information sheet or SIG, including questionnaires and inspections, conducted by Client or another auditor appointed by Client, provided that, unless otherwise required by law, such audits and inspections shall:

5.2.2.1. not take place more than once every calendar year;

5.2.2.2. be requested by Client in writing not less than 14 days prior to the proposed audit date;

5.2.2.3. be conducted during Smarsh's normal business hours; and

5.2.2.4. to the extent legally permitted, be subject to Client's payment of Smarsh's reasonable professional services fees for any dedication of Smarsh resource time to such audit in excess of one hour of resource time.

6. Client Data Incident Management and Notification. Smarsh maintains security incident management policies and procedures and will notify Client without undue delay, but in any event within 48 hours, after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data (including Personal Data), transmitted, stored or otherwise Processed by Smarsh or its Sub-processors (a "**Client Data Incident**"). Smarsh will make reasonable efforts to identify the cause of such Client Data Incident and take those steps Smarsh deems necessary and reasonable to remediate the cause of such a Client Data Incident to the extent the remediation is within Smarsh's reasonable control.

7. Limitation of Liability.

Each party's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement.

8. European Specific Provisions

8.1. GDPR. With effect from May 25, 2018, Smarsh will Process Personal Data in accordance with those GDPR requirements which are directly applicable to Smarsh's provision of its Services.

8.1.1. Data Protection Impact Assessment. With effect from 25 May 2018, upon Client's request, when processing is likely to result in a high risk to the rights and freedoms of natural persons, Smarsh will provide Client with reasonable cooperation and assistance needed to fulfill Client's obligation under the GDPR to carry out a data protection impact assessment related to Client's use of the Services, to the extent the information included in this DPA does not provide sufficient detail. Smarsh will provide reasonable assistance to Client in the cooperation or prior consultation with the Supervisory Authority, to the extent required under the GDPR.

8.1.2. Transfer Mechanisms. As of the effective date of this DPA, Smarsh self-certifies to and complies with the E.U.-U.S. Privacy Shield Framework, as administered by the U.S. Department of Commerce. For transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states to countries which do not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws of the foregoing territories, to the extent such transfers are subject to such applicable Data Protection Laws:

8.1.2.1. Smarsh's EU-U.S. Privacy Shield Framework self-certification applies; and

8.1.2.2. The Standard Contractual Clauses set forth in Exhibit B to this DPA apply, subject to Exhibit B.

List of Exhibits

Exhibit A	DESCRIPTION OF PROCESSING ACTIVITIES
Exhibit B	E.U. STANDARD CONTRACTUAL CLAUSES

The parties' authorized signatories have duly executed this DPA:

On behalf of Client:

Name (written out in full): ____________________

Position: ____________________

Address: ____________________

Signature: ____________________

On behalf of Smarsh, Inc.:

Name: Tricia Juettemeyer

Position: Assistant General Counsel

Address: 851 SW 6th Ave., Suite 800, Portland, OR 97204

Signature: Tricia Juettemeyer (Sep 20, 2018)

EXHIBIT A
DESCRIPTION OF PROCESSING ACTIVITIES

NATURE AND PURPOSE OF PROCESSING

Smarsh will Process Personal Data as necessary to perform the Services purchased by Client under the Agreement, as further specified in any Order Forms, and as further instructed by Client in its use of the Services. Depending on the Services purchased by Client, the purpose of processing is the capture and/or archive of electronic communications for legal, regulatory, e-discovery or similar purposes.

DURATION OF PROCESSING

Smarsh will Process Personal Data for the duration of the Agreement and retain Client Data for a minimum of six months following the termination of the Agreement, unless otherwise agreed upon in writing. Smarsh will destroy Client Data upon the earlier of 12 months following the termination or expiration of the Agreement or upon Client's request

CATEGORIES OF DATA SUBJECTS

Personal Data relating to the following categories of data subjects:

- Prospects, Client, business partners and vendors of Client (who are natural persons)
- Employees or contact persons of Client's prospects, customers, business partners and vendors
- Employees, agents, advisors, of Client (who are natural persons)
- Those users Client authorizes to use the Services

TYPES OF PERSONAL DATA

Smarsh Services receive communication data from Client specified communication applications, platforms or systems. Personal Data may include, but is not limited to the following categories of Personal Data depending on the Services purchased by Client:

- Sender and recipient first name, last name, e-mail address, social media handle, telephone number
- Communication data (such as the content or body of messages sent and received). Communication data may include professional or personal data, information about business transactions or similar kinds of communications
- Log data or activities undertaken by authorized users of the Services (such as messages reviewed, escalated, log in times/dates)
- Business information such as position, employer, contact information

EXHIBIT B
E.U. STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection the data exporter and data importer each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

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

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

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

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

(ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

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

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

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

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses.[3] Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

On behalf of the data importer:

Name (written out in full): Tricia Juettemeyer

Position: Assistant General Counsel

Address: 851 SW 6th Ave., Suite 800, Portland, OR 97204

Signature Tricia Juettemeyer (Sep 20, 2018)……………….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

DATA EXPORTER
Data Exporter is (i) the legal entity identified in the Agreement, including the DPA, and (ii) any Affiliates (as defined in the Agreement) of Client established within the European Economic Area (EEA) that have purchased the Services on the basis of one or more Order Form(s)

DATA IMPORTER
The data importer is Smarsh Inc. and its Affiliates, provider of services which archive electronic communications

DATA SUBJECTS
The personal data transferred concern the following categories of data subjects (please specify):

Data exporter's customers and end-users and those individuals with whom they communicate. The data importer will receive any Personal Data that the data exporter instructs it to process through the Services.

CATEGORIES OF DATA
The Personal Data that the data exporter will transfer to the data importer is determined and controlled solely by the data exporter, but may include some or all of the following categories of data:

- Sender and recipient first name, last name, e-mail address, social media handle, telephone number
- Communication data (such as the content or body of messages sent and received). Communication data may include professional or personal data, information about business transactions or similar kinds of communications
- Log data or activities undertaken by authorized users of the Services (such as messages reviewed, escalated, log in times/dates)
- Business information such as position, employer, contact information

SPECIAL CATEGORIES OF DATA (IF APPROPRIATE)
The personal data transferred concern the following special categories of data (please specify):

Data exporter may process special categories of data via the Services, the extent of which is determined and controlled by
the data exporter in its sole discretion. The data exporter is solely responsible for ensuring the legality of any special categories of data it or its end users choose to process using the Services.

PROCESSING OPERATIONS:
The personal data transferred will be subject to the following basic processing activities (please specify):
Depending on the services purchased, the receipt of communciations data from various platforms or communication channels, as instructed by Client., programmable communication products and services,

DATA EXPORTER

Name:………………………………

Authorised Signature ……………………

DATA IMPORTER

Name: Tricia Juettemeyer

Authorised Signature
Tricia Juettemeyer (Sep 20, 2018)

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

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

Data importer will maintain appropriate technical and organizational measures, which are designed to protect the security, confidentiality and integrity of Client Data (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Client Data), including as appropriate:

- the encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing.

Data Importer will not materially decrease the overall security of the Services during a subscription term.

DATA EXPORTER

Name:………………………………

Authorised Signature ……………………

DATA IMPORTER

Name: Tricia Juettemeyer

Authorised Signature Tricia Juettemeyer (Sep 20, 2018)