DATA PROCESSING ADDENDUM

This DPA is entered into between the Customer (Controller) and SigParser (Processor). SigParser has pre-signed the DPA; Customer's execution of the Agreement shall constitute acceptance of this DPA. The DPA is incorporated into and governed by the terms of the Agreement. The term of this DPA follows the Term of the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the Agreement to the limited extent of such conflict or inconsistency.

1. Definitions

Any capitalized term not defined in this DPA shall have the meaning given to it in the Agreement.

"**Affiliate**"	means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party;
"Agreement"	means the Services and/or Software agreement (i.e., Order and Terms of Service) pursuant to which SigParser provides Services and/or Software to Customer;
"CCPA"	means the California Consumer Privacy Act of 2018, along with its regulations and as amended from time to time;
"Controller"	means the Customer (as defined in the Agreement);
"Data Protection Law"	means all laws and regulations (as amended or replaced), including laws and regulations of the European Union ("EU"), the European Economic Area ("EEA"), their member states and the United Kingdom, applicable to the processing of Personal Data, including the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, the EU GDPR, the UK GDPR, the FDPA, the UK Data Protection Act 2018, the CCPA and any applicable national implementing laws, regulations and secondary legislation relating to the processing of the Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426);
"Data Subject"	shall have the same meaning as in Data Protection Law or means a "Consumer" as that term is defined in the CCPA;
"DPA"	means this Data Processing Agreement together with Exhibits A, B and C, each of which is incorporated herein by reference;
"EU GDPR"	means 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);
"FDPA"	means the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; FDPA) and as amended from time to time;
"Personal Data"	shall have the same meaning as in Data Protection Law;
"Processor"	means Dragnet Technologies, Inc. d/b/a SigParser ("SigParser"), including as applicable any "Service Provider" as that term is defined by the CCPA;
"Restricted Transfer"	means: (i) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and

	(ii) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) a transfer of Personal Data via the Services from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission;
"Services"	means all Services and Software provided to the Controller by the Processor under and as described in the Agreement;
"SCCs"	means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries set out in Exhibit C ("**EU SCCs**"); and (ii) where the UK GDPR applies standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR published at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/ ("**UK SCCs**"); and (iii) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority ("**Swiss SCCs**");
"Sub-Processor"	means any third party (including Processor Affiliates) engaged directly or indirectly by the Processor to process Personal Data under this DPA in the provision of the Services and/or Software to the Controller;
"Supervisory Authority"	means a governmental or government chartered regulatory body having binding legal authority over a party;
"UK GDPR"	means the EU GDPR as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, or such SCC's as may be subsequently adopted or enacted by the UK.

2. **Purpose**

2.1 The Processor has agreed to provide the Services and/or Software to the Controller in accordance with the terms of the Agreement. In providing such Services and/or Software, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

3. **Scope**

3.1 The Processor shall process Personal Data only to the extent necessary to provide the Services and/or Software in accordance with the terms of the Agreement, this DPA and the Controller's instructions as documented in the Agreement and this DPA.

3.2 The parties shall ensure that any natural person acting under the authority of the Controller or the Processor who has access to Personal Data does not process such data except on the instructions from the Controller unless required to do so by any Data Protection Law.

4. **Processor Obligations**

4.1 The Processor may collect, process, or use Personal Data only within the scope of this DPA.

4.2 The Processor confirms that it shall process Personal Data on behalf of the Controller in accordance with the documented instructions of the Controller.

4.3 The Processor shall inform the Controller if, in the Processor's opinion, any of the Controller's instructions breach or may otherwise violate Data Protection Law.

4.4 The Processor shall ensure that all employees, agents, officers, and contractors who handle or have access to Personal Data: (a) are aware of the confidential nature of the Personal Data and are contractually bound or otherwise obligated to keep the Personal Data confidential, and (b) have received training on their responsibilities as a data processor under this DPA.

4.5 The Processor shall implement appropriate technical and organizational procedures to protect Personal Data, considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

4.6 The Processor shall implement technical and organizational measures to ensure a level of security appropriate to the risk, including *inter alia*: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. In assessing the appropriate level of security, the Processor shall consider the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed.

4.7 The Processor shall adhere to the technical and organizational measures set forth in Exhibit B as a minimum security standard. The Controller agrees that these technical and organizational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA, provided such measures are at least equivalent to the technical and organizational measures set forth in Exhibit B and appropriate pursuant to the Processor's obligations in clauses 4.5 and 4.6 above.

4.8 The Controller acknowledges and agrees that, in the course of providing the Services and/or Software to the Controller, it may be necessary for the Processor to access the Personal Data to respond to technical problems or Controller queries and ensure the proper working of the Services or Software. All such access by the Processor will be limited to those purposes.

4.9 Considering the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organizational measures, insofar as this is possible and commercially reasonable, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller's compliance with the Controller's data protection obligations.

4.10 The Processor shall not: (a) sell Personal Data; (b) retain, use, or disclose Personal Data for commercial purposes other than providing the Services and/or Software under the terms of the Agreement; or (c) retain, use, or disclose Personal Data except as permitted by the Agreement.

5. **Controller Obligations**

5.1 The Controller represents and warrants that it shall comply with this DPA and its obligations under Data Protection Law.

5.2 The Controller represents and warrants that it has obtained all necessary consents, permissions, and authorizations necessary to permit the Processor and Sub-Processors to execute their rights or perform their obligations under the Agreement and this DPA.

5.3 All Affiliates of the Controller who use the Services and Software shall comply with the Controller's obligations set forth in this DPA and shall be bound by the DPA as if a party hereto.

5.4 The Controller shall implement appropriate technical and organizational procedures to protect Personal Data, considering the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Controller shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including without limitation: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (c) 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 (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In assessing the appropriate level of security, Controller shall consider the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored, or otherwise processed.

5.5 The Controller acknowledges and agrees that some requests from the Controller, including assisting with audits, inspections, data protection impact assessments, or otherwise providing non-mandatory assistance under this DPA, may result in additional fees or charges. Under these circumstances, the Processor will provide the Controller with an Order form quoting and specifying such fees or charges. If Controller does not accept or execute the Order form, the Processor shall have no obligation to provide such assistance.

6. Sub-Processors

6.1 The Controller acknowledges and agrees that the Processor may engage Sub-Processors in connection with the provision of the Services and/or Software under the Agreement.

6.2 All Sub-Processors who process Personal Data in the provision of the Services or Software to the Controller shall comply with the obligations of the Processor set forth in this DPA.

6.3 The Controller hereby authorizes the Processor to use the Sub-Processors listed on Exhibit C (Annex III) to process Personal Data on behalf of the Controller. If Processor makes any changes to Exhibit C, it will post a notice of such changes here: https://sigparser.com/security/data-processing-sub-processors/ ("List of Sub-Processors"). The Controller acknowledges its duty to periodically review the List of Sub-Processors during the Term and before any Renewal Term.

6.4 If there are any changes to the List of Sub-Processors, Customer shall be deemed to accept the new or replacement Sub-Processor(s) upon any renewal or extension of the Agreement. If Customer does not agree to any such changes, it must not renew or extend the Agreement. If Customer renews or extends the Agreement, this shall be deemed acceptance and authorization of the then-current List of Sub-Processors.

6.5 If Customer objects to changes made to the List of Sub-Processors, (a) Customer shall cease all use of the Services, (b) SigParser may terminate the Agreement, and (c) SigParser may, in its discretion on a pro rata basis, refund any prepaid fees covering the remainder of the Term. No termination of Services pursuant to this section shall constitute a breach of the Agreement.

6.6 All Sub-Processors shall comply with the obligations of the Processor set forth in this DPA. Before any Sub-Processor processes Personal Data, the Processor shall (a) appoint each Sub-Processor under a written contract containing materially the same obligations to those of the Processor in this DPA enforceable by the Processor; and (b) ensure each such Sub-Processor complies with all such obligations.

6.7 The Controller agrees that the Processor and its Sub-Processors may make Restricted Transfers of Personal Data for the purpose of providing the Services to the Controller in accordance with the Agreement. The Processor confirms that such Sub-Processors: (a) are located in a third country or territory recognized by the EU Commission or a Supervisory Authority to have an adequate level of protection; or (b) have entered into the applicable SCCs with the Processor; or (c) have other legally recognized appropriate safeguards in place.

7. Restricted Transfers

7.1 The parties agree that when the transfer of Personal Data from the Controller to the Processor or from the Processor to a Sub-Processor is a Restricted Transfer, it shall be subject to the applicable SCCs.

7.2 The parties agree that the EU SCCs shall apply to Restricted Transfers from the EEA. The EU SCCs shall be deemed entered into (and incorporated into this DPA by reference) and completed as follows:

(i) Module One (Controller to Controller) shall apply where SigParser is processing Customer account data for its own purposes;

(ii) Module Two (Controller to Processor) shall apply where the Customer is a Controller of Customer Data and SigParser is processing Customer Data;

(iii) Module Three (Processor to Processor) shall apply where SigParser is a Processor of Customer Data and SigParser uses a Sub-Processor to process the Customer Data;

(iv) In Clause 7 of the EU SCCs, the optional docking clause will not apply;

(v) In Clause 9 of the EU SCCs Option 2 applies, and the method/time period for giving notice of Sub-Processor changes shall be as set forth in Section 6 of this DPA;

(vi) In Clause 11 of the EU SCCs, the optional language shall not apply;

(vii) In Clause 17 of the EU SCCs, Option 1 applies and the EU SCCs shall be governed by the law of Ireland;

(viii) In Clause 18(b) of the EU SCCs, disputes shall be resolved by the courts of Ireland;

(ix) Annex I of the EU SCCs shall be deemed completed with the information set forth in Exhibit A of this DPA; and

(x) Annex II of the EU SCCs shall be deemed completed with the information set forth in Exhibit B of this DPA.

7.3 The parties agree that the EU SCCs as amended in Section 7.2 shall be adjusted as set forth below where the FDPA applies to any Restricted Transfer:

(i) The Swiss Federal Data Protection and Information Commissioner ("FDPIC") shall be the sole Supervisory Authority for Restricted Transfers exclusively subject to the FDPA;

(ii) Restricted Transfers subject to both the FDPA and the EU GDPR shall be dealt with by the EU Supervisory Authority named in Exhibit A of this DPA;

(iii) The term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;

(iv) Where Restricted Transfers are exclusively subject to the FDPA, all references to the GDPR in the EU SCCs are to be understood to be references to the FDPA;

(v) Where Restricted Transfers are subject to both the FDPA and the EU GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the FDPA insofar as the Restricted Transfers are subject to the FDPA; and

(vi) The Swiss SCCs also protect the Personal Data of legal entities until the entry into force of the revised FDPA.

7.4 The parties agree that the UK SCCs shall apply to Restricted Transfers from the UK and the UK SCCs shall be deemed entered into (and incorporated into this DPA by reference), completed as follows:

(i) Appendix 1 of the UK SCCs shall be deemed completed with the information set forth in Exhibit A of this DPA; and

(ii) Appendix 2 of the UK SCCs shall be deemed completed with the information set forth in Exhibit B of this DPA.

7.5 If any provision of this DPA directly or indirectly contradicts any SCCs, the provisions of the applicable SCCs shall prevail over the terms of the DPA.

8. Data Subject Access Requests

8.1 The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. The Controller acknowledges and agrees that the Processor will process the request to the extent it is lawful and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.

8.2 If the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law. The Controller agrees to and shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request. If the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable or required by law.

9. **Inspection and Audit**

9.1 The Processor will make available to the Controller all information commercially and reasonably necessary to demonstrate compliance with its obligations under this DPA. The Processor will allow for and reasonably contribute to information requests ("inspections") no more than once annually during the term of this DPA, unless there has been a security incident affecting Processor, in which case there may be an additional inspection related to such incident.

9.2 Any inspection under this DPA shall consist of the Processor's most recent reports, compliance certificates, test results and/or extracts or summaries of the foregoing, all of which shall be treated as the Processor's Confidential Information in accordance with the Agreement.

9.3 If, in the reasonable opinion of the Controller, an inspection is not deemed sufficient, the Controller may conduct an audit, no more than once annually, which shall be subject to the following conditions: (a) at the Controller's sole cost and expense; (b) limited in scope to matters specific to the Controller and agreed by the parties in advance; (c) carried out during the Processor's usual business hours and upon reasonable notice which shall be not less than four (4) weeks unless an identifiable material issue has arisen; and (d) conducted in a manner that does not interfere with the Processor's operations or business.

10. **Personal Data Breach**

10.1 The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to Controller's Personal Data ("**Personal Data Breach**").

10.2 The Processor shall take all commercially reasonable measures to: (a) secure the Personal Data of Controller, (b) limit the effects of any Personal Data Breach, and (c) assist the Controller in meeting the Controller's obligations under applicable law.

11. **Compliance, Cooperation and Response**

11.1 The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data which adversely impacts the Controller unless such notification is not permitted under applicable law or a relevant court order.

11.2 The Processor may make copies of and/or retain Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements.

11.3 The Processor shall reasonably assist the Controller in meeting the Controller's obligation to carry out data protection impact assessments (DPIAs), subject to Section 5.5 above and taking into account the nature of the processing, inspections, and other information made available to the Controller under this DPA.

11.4 The Controller shall notify the Processor within a reasonable time of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor under this DPA. The Processor will respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organizational measures to maintain compliance.

11.5 The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a Supervisory Authority in the performance of their respective obligations under this DPA and Data Protection Law.

12. Liability

12.1 To the maximum extent permitted by applicable law, the limitations on liability and exclusions of damages set forth in the Agreement apply to all claims arising from, related to, or associated with this DPA.

12.2 The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-Processors to the same extent the Processor would be liable if performing the services of each Sub-Processor directly under the terms of the DPA, subject to any limitations on liability and exclusions of damages set forth in the Agreement.

12.3 The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its representatives or Affiliates as if such acts, omissions, or negligence had been committed by the Controller itself.

12.4 The Controller shall not be entitled to recover more than once in respect of the same loss or damage arising from, related to, or associated with Processor's breach of this DPA.

13. **Term and Termination**

13.1 The Processor will only process Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically together with termination or expiration of the Agreement.

14. **Deletion and Return of Personal Data**

14.1 The Processor shall at the choice of the Controller, upon receipt of a written request received within 30 days of termination of the Services, delete or return Personal Data to the Controller in accordance with the Agreement. The Processor shall in any event delete all copies of Personal Data in its systems within 90 days of the termination date unless: (a) applicable law or regulations require storage of the Personal Data after termination; or (b) partial Personal Data of the Controller is stored in backups, then such Personal Data shall be deleted from backups up to 1 year after the effective date of termination of the Agreement.

15. General

15.1 This DPA sets forth the entire understanding of the parties with regards to the subject matter set forth herein.

15.2 Should a term or provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected.

15.3 Subject to any requirement of applicable SCCs to the contrary, this DPA shall be governed by the laws of the State of Delaware USA. Subject to any requirement of applicable SCCs to the contrary, any court of competent jurisdiction located in the State of Delaware USA shall have exclusive jurisdiction of all disputes arising from, related to, or associated with this DPA. If the foregoing choices of law and forum are declared invalid, then this DPA shall be governed by the law of Ireland, and the courts of Ireland shall have exclusive jurisdiction of all disputes arising from, related to, or associated with this DPA.

12.4 The parties agree that this DPA is incorporated into the Agreement.

Exhibit A

List of Parties, Description of Processing and Transfer of Personal Data, Competent Supervisory Authority

MODULE TWO: CONTROLLER TO PROCESSOR

A. LIST OF PARTIES

The Controller:

means the Customer (as identified in the Agreement)	
Address:	As set forth for the Customer in the Agreement.
Contact person's name, position and contact details:	As provided by the Customer in the Agreement or the account Customer established for its Order.
Activities relevant to the data transferred under the SCCs:	Use of the Services and/or Software.
Signature and Date:	By entering into the Agreement, the Controller is deemed to have signed the SCCs and Annexes incorporated into this DPA, as of the Effective Date of the Agreement. If Customer requires an execution copy for compliance or regulatory purposes, it should download this DPA, and sign/date below: _____ Date: _____
Role:	Data Exporter.
Name of Representative (if applicable):	Any UK or EU representative named in the Controller's privacy policy, Services account, or on Customer's website.

The Processor:

means Dragnet Technologies, Inc. ("SigParser")	
Address:	310 S Twin Oaks Valley Road #107 - 337 San Marcos, CA 92078-4387
Contact Person name, position and contact details:	Chris Landry, Sales and Customer Success, clandry@sigparser.com Cris Campbell, GDPR Manager cris@sigparser.com

Activities relevant to the data transferred under the SCCs:	SigParser provides Services/Software to the Controller as described in the Agreement, thereby processing Personal Data upon the instructions of the Controller.
Signature and Date:	*Chris Landry* Date: November 15, 2022
Role:	Data Importer (Processor)
Name of GDPR Representative:	IT Governance Europe Ltd Attn: Loredana Tassone eurep@itgovernance.eu

B. DESCRIPTION OF PROCESSING AND TRANSFERS

Categories of data subjects:	Employees, agents, advisors, consultants, and contractors of the Controller (who are natural persons). Users, Affiliates and other participants or persons authorized by the Controller to access or use the Services in accordance with the terms of the Agreement. Prospects, customers, clients, contacts, associates and vendors of the Controller (who are natural persons) and individuals with whom those end users communicate with by email and/or other messaging media. Employees or contact persons of Controller's prospects, customers, clients, business associates and vendors. Suppliers, vendors and service providers of the Controller. Other individuals to the extent identifiable in the context of emails of their attachments or in archiving content.
Categories of Personal Data:	The Controller submits Personal Data to the Services, the nature and extent of which is determined and managed by the Controller. The Personal Data may include but is not limited to: ● Names, titles, contact details, phone numbers, and email addresses of users of the Services. ● Unique identifiers such as username, account number or password. ● Personal Data derived from a user's use of the Services such as records and business intelligence information. ● Personal Data within emails and messaging content which identifies or may reasonably be used to identify data subjects. ● Meta data including sent, to, from, date, time, subject, which may include Personal Data. ● Data concerning business affiliations, titles, positions, social media, and profession. ● File attachments that may contain Personal Data. ● Survey, feedback and assessment messages.

	● Information offered by users as part of support enquiries or for Customer service. ● Other data added by the Controller from time to time
Sensitive Data:	No sensitive data will be processed or transferred and shall not be contained in the content of or attachments to, emails. Controller agrees that it shall not transfer, supply, or upload any sensitive data or special categories of data to the Services.
Frequency of the Processing and Transfer (whether Customer Data is transferred on a one-off or continuous basis):	When Controller is using the Services, the processing is on a continuous basis for the duration of the Agreement.
Nature of the Processing:	• Personal Data will be processed to the extent necessary to provide the Services in accordance with the Agreement and the Controller's instructions. • Processing operations include but are not limited to parsing of emails that Controller links and/or uploads to the Services. These operations relate to all aspects of Personal Data processed. • Technical support, problem diagnosis and error correction to ensure the proper operation of the Services and to identify, analyze, and resolve technical issues generally in the provision of the Services and specifically in answer to a controller query. This operation may relate to all aspects of Personal Data processed but will be limited to metadata where possible. • Virus, anti-spam, malware, and security operations in accordance with the Services provided and Agreement. • URL scanning for the purposes of providing targeted threat protection and similar activities. This operation relates to attachments and links in emails and relates to any personal data within those attachments or links which could include all categories of Personal Data.
Purpose(s) of the Data Transfer and further processing:	The Controller transfers email data so that it can be processed or "parsed" in ways that enable the Controller to gain business information and insights. Upon receipt by the Services or Software, some Personal Data may be transferred to Sub-Processors that provide services to the Processor as part of the Services provided by the Processor to the Controller.
Period for which the Personal Data will be retained:	As specified in the Agreement, subject to Section 14 of the DPA.
For Transfers to Sub-Processors, specify subject matter, nature and duration of the processing:	The Sub-Processor list (Exhibit C, Annex III) specifies the Personal Data processed by each Sub-Processor and the services provided by each Sub-processor. ■ The Services are hosted by Amazon Web Services (AWS). The AWS hosting is continuous and

	sub-processing occurs for so long as the Services account is active. This sub-processing is therefore continuous. ■ Email addresses *only* are sub-processed for the Services by Clearout for purposes of verifying that the email address is valid. This verification consists of a single query and is not continuous with the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify Supervisory Authority/ies (e.g. in accordance with Clause 13 of the SCCs)	Where the EU GDPR applies, the Data Protection Commission (DPC) of Ireland Where the UK GDPR applies, the UK Information Commissioner's Office (ICO). Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner (FDPIC).

MODULE THREE: PROCESSOR TO PROCESSOR

A. LIST OF PARTIES

The Data Exporter: is SigParser

The Data Importers: are the Sub-Processors set forth in Exhibit C (Annex III) which contains the name, address, contact details and activities relevant to the data transferred to each Data Importer.

B. DESCRIPTION OF PROCESSING AND TRANSFERS

The List of Sub-Processors (https://sigparser.com/security/data-processing-sub-processors/) includes the information about the processing and transfers of the Personal Data, for each Data Importer:

- categories of Data Subjects
- categories of Personal Data
- the nature of the processing
- the purposes of the processing

Personal Data is processed by each Data Importer:

- on a continuous basis during provision of the Services
- to the extent necessary to provide the Services in accordance with the Agreement and the Data Exporter's instructions.
- for the duration of the Agreement and subject to clause 14 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

The competent Supervisory Authority of the Data Exporter shall be:

- Where the EU GDPR applies, the Data Protection Commission of Ireland;
- Where the UK GDPR applies, the UK Information Commissioner's Office (ICO).
- Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner (FDPIC).

Exhibit B

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

This Exhibit describes the technical and organisational measures the Processor has implemented to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. For security reasons, the Processor does not publicly disclose the entire array or nature of its security measures, or all the measures it takes to protect Personal Data. Upon request, the Processor will provide the Controller with more detailed descriptions of these measures; all such descriptions shall be Confidential Information. Where applicable this Exhibit B will serve as Annex II to the SCCs.

A. SECURITY PROGRAM & OTHER MEASURES

SigParser maintains and administers a comprehensive information security program, including policies and procedures ("Security Program"), to ensure the confidentiality, security, integrity, and availability of controller/Customer data, the Services, and SigParser's internal systems. The Security Program includes administrative, technical, and physical safeguards (including reasonable disposal and degaussing measures) to safeguard such data, the Services, and SigParser's internal systems against unauthorized access, use, disclosure, modification, unavailability, and deletion. SigParser operates and maintains the Security Program in accordance with applicable laws and software industry best practices.

SigParser's Security Program includes, but is not limited to, the following: (a) no less than once annually, mandatory security awareness training for all SigParser personnel (including management and consultants), which includes (i) training on how to implement and comply with its information security program; and (ii) promoting a culture of security awareness; (b) use of up-to-date cybersecurity technologies and practices, including firewalls, multi-factor authentication and other access controls and monitoring (e.g., establishment of appropriate logs and reports regarding access, as well as *encryption* of controller/Customer Data in transit and at rest); (c) background checks on employees, consultants and other personnel with access to controller/Customer Data, the Services, and SigParser's internal systems; (d) restriction on access to and use and copying of controller/Customer Data on a "need-to-know" basis and only at or from authorized locations; (e) regular monitoring of the transport and storage of controller/Customer Data and associated Services or SigParser internal systems; (f) regular penetration testing and vulnerability assessments of SigParser's systems, prompt remediation of any found deficiencies and prompt notification to Customer with detail to allow Customer to take action, if any, to mitigate any adverse impact on Customer, Customer's systems, and data subjects; (g) due diligence and regular monitoring of consultants and subcontractors performing services, working on SigParser's systems/facilities or working on Customer's systems/facilities; (h) logical segregation of controller/Customer Data from other information and/or data accessed, stored or hosted by SigParser (or any of its subcontractors or other third party), including the *encrypted storage* of Controller/Customer Data; (i) ethical walls and internal procedures when providing services to Customer or any third party to prevent breach of confidentiality and to avoid any conflicts of interest; (j) promptly upon termination of employment or engagement, as applicable, of SigParser personnel with access to the Services, SigParser's internal systems, controller/Customer Data and/or Customer's systems, disabling all such access and (if applicable) notifying Customer to disable any Customer-controlled access methods or permissions with respect to such terminated personnel; and (k) continuous and ongoing SOC2 Type II auditing.

B. CERTIFICATIONS

SOC2 Type II Certification

C. ADDITIONAL INFORMATION

SigParser's technical and organizational security measures are comprehensively described in (1) System and Organization Controls (SOC) 2 Type I Report (dated April 12, 2021), and (2) the SigParser Security Overview (dated September 13, 2021). SigParser has provided or made available to Controller/Customer the foregoing documents.

D. DATA STORAGE DETAILS

RDS Servers

Most data is stored on AWS RDS Postgresql databases version 10.6.
Auto minor version upgrade is enabled.
Backup: 7 days of full backups. Ability to do a point in time recovery to any minute of day.
Backups are tested every two months.
Termination protection enabled on production databases.
Downtime in case of complete server failure: 60 minutes to recover from backups.
Data stored encrypted at rest.

RDS Data Isolation

A single database server can store the data for several SigParser controllers/Customers.
Each controller/Customer has its own isolated database file.
Data for two controllers/Customers is never mixed in a single database.
Provides an option to give controllers/Customers a dedicated server for their contact data.

VPC Firewall Restrictions

No inbound open internet access allowed to the databases.
Specific VPC Subnets are defined to have access.
Development and build servers cannot access the production resources; these are isolated using security groups from the development resources.

S3 Storage for User Data (encrypted at rest)

PST Files -- PST files can be uploaded to SigParser for processing. It can take days to process these. SigParser has an automatic lifecycle configured in S3 to delete any PST file uploaded within 30 days regardless of whether the file was processed or not.

Other User Files -- User files such as CSV exports and image uploads for sending emails thru SigParser can also be stored in S3. These do not have an automatic lifecycle configured but will all be deleted when the account or team is deleted.

Email Storage

SigParser stores the metadata for an email but does not store the actual email bodies or attachments. SigParser must store some data about the emails from email systems in order to drive the user interface. SigParser stores the following data on each email it processes:

Subject (optional)
To
From
Date
CC
Message IDs
Folder IDs and folder details like folder names
Attachment names and sizes
Signature Details (phone numbers, titles, locations, Twitter URLs and other meta data).

SigParser *DOES NOT* store:

Email body text (plain or HTML)
Email attachment contents
Keywords

E. TRANSFERS TO SUB-PROCESSORS

The SigParser Services use only two Sub-Processors (AWS and Clearout) to which Customer's Personal Data is transferred for purposes of processing. SigParser and AWS have executed a DPA and any transfers are covered by the SCCs. SigParser and Clearout have executed a Sub-Processing Agreement consistent with this DPA and the SCCs.

Exhibit C

EU Standard Contractual Clauses

Note: if non-EU SCCs apply to this DPA, the information and designations provided below shall be used to fill those SCCs in the appropriate places and incorporated therein.

SECTION I

Clause 1 - Purpose and Scope

(a) The purpose of these standard contractual clauses ("**EU SCCs**") 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 ("**EU GDPR**") for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies ("**Entity/ies**") transferring the personal data, as listed in Annex I.A (each a "**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 EU SCCs, as listed in Annex I.A (each a "**Data Importer**")

(iii) have agreed to these EU SCCs.

(c) These EU SCCs apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these EU SCCs containing the Annexes referred to therein forms an integral part of these EU SCCs.

Clause 2 - Effect and Invariability of the EU SCCs

(a) These EU SCCs set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of the EU GDPR and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of the EU GDPR, 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 EU SCCs in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these EU SCCs or prejudice the fundamental rights or freedoms of data subjects.

(b) These EU SCCs are without prejudice to obligations to which the Data Exporter is subject by virtue of the EU GDPR.

Clause 3 - Third-party Beneficiaries

(a) Data subjects may invoke and enforce these EU SCCs, as third-party beneficiaries, against the Data Exporter and/or Data Importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under the EU GDPR.

Clause 4 - Interpretation

(a) Where these EU SCCs use terms that are defined in the EU GDPR, those terms shall have the same meaning as in the EU GDPR.

(b) These EU SCCs shall be read and interpreted in the light of the provisions of the EU GDPR.

(c) These EU SCCs shall not be interpreted in a way that conflicts with rights and obligations provided for in the EU GDPR.

Clause 5 - Hierarchy

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

Clause 6 - Description of the Transfer(s)

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

Clause 7 – Optional - Docking Clause

(a) An Entity that is not a Party to these EU SCCs may, with the agreement of the Parties, accede to these EU SCCs at any time, either as a Data Exporter or as a Data Importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding Entity shall become a Party to these EU SCCs and have the rights and obligations of a Data Exporter or Data Importer in accordance with its designation in Annex I.A.

(c) The acceding Entity shall have no rights or obligations arising under these EU SCCs 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 EU SCCs.

MODULE TWO: Transfer Controller to Processor

8.1 Instructions

(a) The Data Importer shall process the personal data only on documented instructions from the Data Exporter. The Data Exporter may give such instructions throughout the duration of the contract.

(b) The Data Importer shall immediately inform the Data Exporter if it is unable to follow those instructions.

8.2 Purpose Limitation

The Data Importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the Data Exporter.

8.3 Transparency

On request, the Data Exporter shall make a copy of these EU SCCs, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the Data Exporter may redact part of the text of the Appendix to these EU SCCs prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This EU SCCs is without prejudice to the obligations of the Data Exporter under Articles 13 and 14 of the EU GDPR.

8.4 Accuracy

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

8.5 Duration of Processing and Erasure or Return of Data

Processing by the Data Importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the Data Importer shall, at the choice of the Data Exporter, delete all personal data processed on behalf of the Data Exporter and certify to the Data Exporter that it has done so, or return to the Data Exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with these EU SCCs. 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 EU SCCs 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 a Personal Data Breach. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the Data Exporter. In complying with its obligations under this paragraph, the Data Importer shall at least implement the technical and organisational measures specified in Annex II. The Data Importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The Data Importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a Personal Data Breach concerning personal data processed by the Data Importer under these EU SCCs, 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 the EU GDPR, 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 Sensitive Data, the Data Importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward Transfers

The Data Importer shall only disclose the personal data to a third party on documented instructions from the Data Exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the Data Importer or in another third country, "**Onward Transfer**") if the third party is or agrees to be bound by these EU SCCs, under the appropriate Module, or if:

(i) the Onward Transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of the EU GDPR that covers the Onward Transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of the EU GDPR 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 EU SCCs, 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 EU SCCs.

(b) The Parties shall be able to demonstrate compliance with these EU SCCs. 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 EU SCCs and at the Data Exporter's request, allow for and contribute to audits of the processing activities covered by these EU SCCs, 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.

MODULE THREE: Transfer Processor to Processor

8.1 Instructions

(a) The Data Exporter has informed the Data Importer that it acts as Processor under the instructions of its Controller(s), which the Data Exporter shall make available to the Data Importer prior to processing.

(b) The Data Importer shall process the personal data only on documented instructions from the Controller, as communicated to the Data Importer by the Data Exporter, and any additional documented instructions from the Data Exporter. Such additional instructions shall not conflict with the instructions from the Controller. The Controller or Data Exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The Data Importer shall immediately inform the Data Exporter if it is unable to follow those instructions. Where the Data Importer is unable to follow the instructions from the Controller, the Data Exporter shall immediately notify the Controller.

(d) The Data Exporter warrants that it has imposed the same data protection obligations on the Data Importer as set out in the contract or other legal act under Union or Member State law between the Controller and the Data Exporter.

8.2 Purpose Limitation

The Data Importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B., unless on further instructions from the Controller, as communicated to the Data Importer by the Data Exporter, or from the Data Exporter.

8.3 Transparency

On request, the Data Exporter shall make a copy of these EU SCCs, 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 personal data, the Data Exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

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 rectify or erase the data.

8.5 Duration of Processing and Erasure or Return of Data

Processing by the Data Importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the Data Importer shall, at the choice of the Data Exporter, delete all personal data processed on behalf of the Controller 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 EU SCCs. 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 EU SCCs 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 (hereinafter "**Personal Data Breach**"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. 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 or the Controller. In complying with its obligations under this paragraph, the Data Importer shall at least implement the technical and organisational measures specified in Annex II. The Data Importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The Data Importer shall grant access to the 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 EU SCCs, the Data Importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The Data Importer shall also notify, without undue delay, the Data Exporter and, where appropriate and feasible, the Controller 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 data breach, including 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 the EU GDPR, in particular to notify its Controller so that the latter may in turn 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 Sensitive Data, the Data Importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward Transfers

The Data Importer shall only disclose the personal data to a third party on documented instructions from the Controller, as communicated to the Data Importer by 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, ("**Onward Transfer**") if the third party is or agrees to be bound by these EU SCCs, under the appropriate Module, or if:

(i) the Onward Transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of the EU GDPR that covers the Onward Transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of the EU GDPR;

(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 SCCs, in particular purpose limitation.

8.9 Documentation and Compliance

The Data Importer shall promptly and adequately deal with enquiries from the Data Exporter or the Controller that relate to the processing under these SCCs.

(a) The Parties shall be able to demonstrate compliance with these SCCs. In particular, the Data Importer shall keep appropriate documentation on the processing activities carried out on behalf of the Controller.

(b) The Data Importer shall make all information necessary to demonstrate compliance with the obligations set out in these EU SCCs available to the Data Exporter, which shall provide it to the Controller.

(c) The Data Importer shall allow for and contribute to audits by the Data Exporter of the processing activities covered by these SCCs, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the Data Exporter requests an audit on instructions of the Controller. In deciding on an audit, the Data Exporter may take into account relevant certifications held by the Data Importer.

(d) Where the audit is carried out on the instructions of the Controller, the Data Exporter shall make the results available to the Controller.

(e) 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.

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

MODULE TWO: Transfer Controller to Processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION 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 30 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 EU SCCs, 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 EU SCCs.

(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.

MODULE THREE: Transfer Processor to Processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The Data Importer has the Controller's general authorization for the engagement of sub-processor(s) from an agreed list. The Data Importer shall specifically inform the Controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Controller 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 Controller with the information necessary to enable the Controller to exercise its right to object. The Data Importer shall inform the Data Exporter of the engagement of the sub-processor(s).

(b) Where the Data Importer engages a sub-processor to carry out specific processing activities (on behalf of the Controller), 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 EU SCCs, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this EU SCCs, 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 EU SCCs.

(c) The Data Importer shall provide, at the Data Exporter's or Controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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

MODULE TWO: Transfer Controller to Processor

(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 the EU GDPR. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the Data Importer shall comply with the instructions from the Data Exporter.

MODULE THREE: Transfer Processor to Processor

(a) The Data Importer shall promptly notify the Data Exporter and, where appropriate, the Controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the Controller.

(b) The Data Importer shall assist, where appropriate in cooperation with the Data Exporter, the Controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under the EU GDPR or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the Data Importer shall comply with the instructions from the Controller, as communicated by 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.

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these EU SCCs, 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 the EU GDPR.

(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

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

(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 EU SCCs.

(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 EU SCCs.

(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 EU SCCs. 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 the EU GDPR 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 EU SCCs, 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

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

(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 the EU GDPR as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the Data Exporter is not established in an EU Member State but falls within the territorial scope of application of the EU GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the EU GDPR: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of the EU GDPR is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the Data Exporter is not established in an EU Member State, but falls within the territorial scope of application of the EU GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the EU GDPR: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these EU SCCs in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The Data Importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these EU SCCs. 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 EU SCCs

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

(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 EU SCCs. 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 the EU GDPR, are not in contradiction with these EU SCCs.

(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 EU SCCs, 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 EU SCCs.

(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 EU SCCs 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). [For Module Three: The Data Exporter shall forward the notification to the Controller.]

(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 EU SCCs, 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 [for Module Three:, if appropriate in consultation with the Controller]. 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 [for Module Three: the Controller or] 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 EU SCCs. 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

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

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 EU SCCs; 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 EU SCCs in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

For Module Three: The Data Exporter shall forward the notification to the Controller.

(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.). [For Module Three: The Data Exporter shall forward the information to the Controller.]

(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 EU SCCs.

15.2 Review of Legality and Data Minimization

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

(b) The Data Importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The Data Exporter shall make the assessment available to the Controller.]

(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 EU SCCs and Termination

(a) The Data Importer shall promptly inform the Data Exporter if it is unable to comply with these EU SCCs, for whatever reason.

(b) In the event that the Data Importer is in breach of these EU SCCs or unable to comply with these EU SCCs, 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 EU SCCs, where:

(i) the Data Exporter has suspended the transfer of personal data to the Data Importer pursuant to paragraph (b) and compliance with these EU SCCs 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 EU SCCs; or

(iii) the Data Importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these EU SCCs.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the Controller] of such non-compliance. Where the contract involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) For Modules Two and Three:

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.

(e) Either Party may revoke its agreement to be bound by these EU SCCs where (i) the European Commission adopts a decision pursuant to Article 45(3) of the EU GDPR that covers the transfer of personal data to which these EU SCCs apply; or (ii) the EU GDPR 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 the EU GDPR.

Clause 17 - Governing law

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

OPTION 2 (for Modules Two and Three): These EU SCCs shall be governed by the law of the EU Member State in which the Data Exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18 - Choice of Forum and Jurisdiction

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

(a) Any dispute arising from these EU SCCs 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.

Annex I

List of Parties, Description of Transfer and Competent Supervisory Authority

See Exhibit A of the DPA.

Annex II

Technical and Organisational Measures (Including Technical and Organisational Measures to Ensure the Security of the Data)

See Exhibit B of the DPA.

ANNEX III

LIST OF SUB-PROCESSORS

As of the Effective Date of the Agreement, the Controller has authorized the Processor's use of the following Sub-Processors:

1. **Amazon Web Services:** contact information can be found at AWS Support: https://aws.amazon.com/contact-us/. AWS hosts the SigParser cloud Services. When establishing its SigParser account, Customer may choose between the Services hosted by AWS in the United States or European Union (Frankfurt, Germany).

2. **Kintegra, Inc. d/b/a Clearout:** 2035 Sunset Lake Road, Suite B-2, Newark, DE 19702, phone (302) 440-1582. Clearout sub-processes parsed email addresses to verify that those addresses are active. If Customer chooses to have the SigParser Services hosted by AWS Frankfurt, Clearout's sub-processing services are also hosted by AWS Frankfurt.